SOBRE LA PRUEBA DE LA CONJETURA DE KEMNITZ

NIDIA YADIRA CAICEDO BRAVO

Universidad del Valle
Facultad de Ciencias Naturales y Exactas
Departamento de Matemáticas
Maestría en Ciencias Matemáticas
Santiago de Cali
2011

SOBRE LA PRUEBA DE LA CONJETURA DE KEMNITZ

NIDIA YADIRA CAICEDO BRAVO

Trabajo de grado presentado como requisito para optar al título de Magíster en Ciencias Matemáticas

Dirigido por
Carlos Alberto Trujillo, Ph. D.

Universidad del Valle
Facultad de Ciencias Naturales y Exactas
Departamento de Matemáticas
Maestría en Ciencias Matemáticas
Santiago de Cali
2011

FACULTAD DE CIENCIAS NATURALES Y EXACTAS

ACTA DE SUSTENTACIÓN DEL TRABAJO DE INVESTIGACIÓN DE MAESTRIA EN CIENCIAS-MATEMÁTICAS

Jurado conformado por los doctores:

Dr. ISMAEL GUTIÉRREZ, Universidad del Norte - Barranquilla
Dr. GUILLERMO ORTIZ R., Universidad del Valle

El día 28 de Marzo de 2011 a las 2:00 PM se llevó a cabo la sustentación del Trabajo de Investigación **"SOBRE LA PRUEBA DE LA CONJETURA DE KEMNITZ"**, presentado por la estudiante **NIDIA YADIRA CAICEDO BRAVO,** código 0703705, Plan 7179, candidata a grado para la próxima ceremonia.

RESULTADO DE LA EVALUACIÓN:

(✓) APROBADA
( ) MERITORIA
( ) LAUREADA

Regístrese esta calificación.

( ) REPROBADA: La estudiante debe matricularse en esta actividad

( ) PENDIENTE: La estudiante debe acoger las recomendaciones del jurado y presentar nuevamente el documento ante el Director de Tesis. ( ) Requiere. ( ) No requiere nueva sustentación.

El plazo para nueva sustentación y/o presentación del documento es de: _____

OBSERVACIONES

Santiago de Cali, 28 de Marzo de 2011

ISMAEL GUTIÉRREZ
Jurado

GUILLERMO ORTIZ R.
Jurado

CARLOS ALBERTO TRUJILLO
Director de Tesis

JOSÉ RAÚL QUINTERO
Coordinador de la Sustentación
Dir. Posgrado en Ciencias-Matemáticas

A la memoria de mi padre Jairo.
A mi madre Lilia y mis hermanos Ayda Lilia y
Jairo Adrián.

AGRADECIMIENTOS

En esta oportunidad, quiero agradecerles a las personas que han sido especiales y que se suman a celebrar este triunfo tan importante en mi vida, que de una u otra manera con su apoyo y entusiasmo hicieron de este proyecto una experiencia de vida.

Agradezco a DIOS por mostrarme el camino e iluminarme a tomar decisiones acertadas. A mi familia, quienes son mi fuerza, motor e impulso, a mi madre, Lilia Bravo, mis hermanos, Ayda Lilia y Jairo Adrián.

También, ocupa un lugar privilegiado, la Universidad del Valle, por darme la oportunidad de pertenecer a ella y realizar estudios de nivel superior. A los docentes del Departamento de Matemáticas, en particular a los maestros que contribuyeron en mi formación, durante mi permanencia en el Programa de Maestría en Ciencias Matemáticas.

Al Dr. Carlos Alberto Trujillo, docente de la Universidad del Cauca y director de este trabajo de investigación, por compartir y ser una mano amiga para profundizar estudios en la Teoría de Números y llevar a buen término este trabajo.

Al profesor Carlos Alexis Gómez y mi compañero Jhonny C. Gómez, por sus aportes pertinentes, explicaciones y discusiones referentes para este trabajo.

Finalmente, a mis compañeros por hacer cada día de esta magna experiencia un momento para recordar toda la vida.

CONTENIDO

RESUMEN

En este trabajo realizamos una monografía sobre la Prueba de la Conjetura de Kemnitz, basándonos en el artículo *On Kemnitz'conjeture concerning lattice-points in the plane.* Ramanujan J., *13:333-337, 2007* de *Christian Reiher*. Esta conjetura surgió del problema unidimensional que demostraron, en 1961, P. Erdös, A. Ginzburg y A. Ziv [14]; el cual dice que: "toda secuencia de $(2n-1)$ enteros, contiene una subsecuencia de tamaño n cuya suma de elementos es divisible entre n."Este resultado se ha demostrado por diversos caminos, utilizando herramientas combinatorias y algebraicas. Además, este problema fue extendido a varias dimensiones; por ejemplo, el caso bidimensional que consiste en determinar el menor entero $s(n,2)$ tal que cualquier secuencia con s elementos de $\mathbb{Z}_n \oplus \mathbb{Z}_n$ contiene una subsecuencia de tamaño n, cuya suma de elementos es congruente con cero módulo n. En el año de 1983, A. Kemnitz [24] conjeturó que $s(n,2) = 4n-3$, para todo n. Esta conjetura fue un problema abierto durante 20 años hasta que, en Octubre de 2003, C. Reiher en [37] probó que es verdadera.

Se inicia este trabajo con una amplia revisión bibliográfica de algunas demostraciones del Teorema de P. Erdös, A. Ginzburg y A. Ziv, luego estudiamos algunos casos particulares del valor de la función $s(n,2)$ en el cual comprobamos que en efecto para estos casos la conjetura es verdadera; más adelante hacemos una revisión de ciertas cotas importantes que están muy cercanas al valor de dicha función pues los argumentos usados para las demostraciones de las mismas están relacionados con las pruebas del Teorema de P. Erdös, A. Ginzburg y A. Ziv y la prueba de la Conjetura de Kemnitz (hoy Teorema de Reiher) y por último reconstruimos en detalle la prueba de la Conjetura de Kemnitz, dada por C. Rehier en el artículo que mencionamos antes.

El estudio de los problemas de suma cero es relevante ya que es un tema de frontera en la investigación actual, tiene relación con otras áreas de la Teoría de Números Aditiva como los conjuntos suma y los cubrimientos de enteros; además tiene aplicaciones en la Teoría de Ramsey, en particular en el estudio sobre los números Ramsey de suma cero y también tienen relación con la Teoría de Códigos.

INTRODUCCIÓN

Consideremos el siguiente "juego matemático": con una baraja de M cartas, M un entero positivo, cualquier número de jugadores puede participar; se elige uno de ellos como representante que lo llamaremos tallador. Uno de los jugadores toma una carta y la muestra a los demás para tener en cuenta el valor numérico de dicha carta, digamos que su valor es n. Se introduce de nuevo la carta en la baraja y el tallador combina ahora todas las cartas y empieza a repartir las cartas sobre una mesa, cara arriba una por una en un intervalo de tiempo acordado, por ejemplo de un minuto; un jugador gana el juego seleccionando k cartas, $1 \leq k \leq M$, que están sobre la mesa, tales que la suma de sus valores numéricos sea divisible entre n.

Después de esta breve descripción del juego, las preguntas que surgen ahora son las siguientes:

1. ¿Es siempre posible ganar el juego?
2. ¿Se pueden repartir todas las cartas y no obtener solución alguna?
3. ¿Cuál es el menor número M de cartas que se necesitan para que haya un ganador?

La respuesta a las preguntas anteriores es que el juego si tiene solución siempre y cuando el número M total de las cartas en la baraja sea suficientemente grande en comparación con el módulo n seleccionado [10].

Ahora bien, si cambiamos las reglas del juego y agregamos un requisito adicional; para ganar el juego en lugar de recoger cualquier número de cartas cuya suma es divisible entre n, hay que seleccionar con precisión n cartas tales que la suma

de sus valores numéricos sea divisible entre n. De nuevo nos podemos hacer las anteriores preguntas y entonces tenemos que si es posible ganar el juego, no es necesario repartir todas las cartas para obtener solución alguna siempre y cuando el número total de carta sea suficientemente grande, trivialmente nos podemos dar cuenta que al menos se deben repartir n cartas y el menor número M de cartas que se necesitan para que exista un ganador es $M = 2n - 1$.

El juego en el que se cambian las reglas nos describe un resultado matemático que fue probado en 1961 por P. Erdös, A. Ginzburg y A. Ziv [14], quienes inician el estudio de los problemas de suma cero que son cierta clase de problemas combinatorios y a partir de esto se establece la fundamentación de la Teoría de Suma Cero; este resultado nos dice que: "toda secuencia con $(2n - 1)$ enteros contiene una subsecuencia de tamaño n cuya suma de elementos es divisible entre n". Resultado que se conoce con el nombre de Teorema de Erdös, Ginzburg y Ziv y tiene varias extensiones y generalizaciones, por ejemplo, a partir de dicho teorema surge una nueva forma de representar los elementos de grupos abelianos como suma de términos de una secuencia dada; en 1961, R. Eggleton junto con P. Erdös en [12] presentan condiciones sobre grupos abelianos aditivos que posean secuencias que representen los elementos del grupo. En 1967, H. Mann en [25] demuestra que dada una secuencia de tamaño $2p - 1$ en un grupo de orden p primo, todo elemento del grupo se representa como suma de los elementos de una subsecuencia de tamaño p. De la misma manera, W. Gao en [16] muestra un refinamiento de este teorema.

Años después, P. Erdös y H. Davenport formulan el siguiente problema: dado un grupo finito abeliano G, determinar el menor entero positivo t tal que toda secuencia en G de tamaño por lo menos t posea una subsecuencia que represente el elemento neutro de G. Ese entero t es conocido como la Constante de Davenport de G, se denota $D(G)$ y es muy estudiada por varios autores; además podemos observar que está relacionada con la descripción del primer juego. En 1968, J. Olson en [31] calculó el valor exacto para el p-grupo $\mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_r}}$ donde p es un entero primo.

En 1973, H. Harborth [23] se interesa por el estudio del problema multidimensional que consiste en encontrar el menor número entero $s(n, d)$ tal que cualquier secuencia de $\mathbb{Z}_n^d$ con s elementos contiene una subsecuencia de tamaño n y suma cero. H. Harborth probó las cotas triviales $(n-1)2^d+1 \leq s(n, d) \leq (n-1)n^d+1$. y que si $n = 2^a3^b$ y $d = 2$ entonces cualquier secuencia de $4n - 3$ elementos en $\mathbb{Z}_n \oplus \mathbb{Z}_n$ contiene una subsecuencia de tamaño n y suma cero.

A. Kemnitz [24], en 1983, obtuvo el mismo resultado de H. Harborth para el caso de $n = 2^a3^b5^c7^d$ y conjeturó que es verdadero para cualquier entero positivo n, es decir que $s(n, 2) = 4n-3$; para la demostración de los casos de $n = 3, 5, 7$ utiliza la

función $g(n,2)$, la cual denota el menor entero positivo g tal que cada subconjunto de cardinalidad g del grupo $\mathbb{Z}_n \oplus \mathbb{Z}_n$ contiene un subconjunto de cardinalidad n cuya suma es cero. Kemnitz (Extremal probleme für Gitterpunkte, Ph. D. Thesis, Technische Universität Braunschweig,1982) probó que $g(n,2) = 2n-1$ para los casos de $n = 3, 5, 7$.

La conjetura de Kemnitz fue un problema que permaneció abierto durante 20 años hasta que en Octubre de 2003 Christian Reiher [37] probó que es verdadera.

C. Reiher nació en el año de 1984, de nacionalidad alemana, ha sido el participante con mayor éxito en la historia de las Olimpiadas de Matemáticas Internacionales, obteniendo cuatro medallas de oro en los años 2000 al 2003 y una medalla de bronce en 1999. Después de terminar su bachillerato prueba la Conjetura de Kemnitz, un importante problema en la Teoría de Suma Cero; terminó su carrera en Matemáticas en Ludwig Maximilian Universidad de Munich y se doctoró en la Universidad de Rostock en Febrero de 2010.

Actualmente existen varias demostraciones del Teorema de Erdös, Ginzburg y Ziv, en el primer capítulo de este trabajo presentamos cuatro demostraciones de este resultado con el objetivo de analizar los argumentos que se usan para la demostración y notar que existe relación con los argumentos usados para la prueba de la Conjetura de Kemnitz (hoy en día Teorema de Reiher); la primera demostración está basada en el Teorema de Cauchy-Davenport [29], el cual tiene muchas aplicaciones en Teoría Aditiva de Números. En la segunda demostración usamos el Teorema de Chevalley-Warning [9], que trata sobre el número de soluciones de sistemas de ecuaciones con coeficientes en un campo finito; este teorema es el argumento principal para la prueba de la Conjetura de Kemnitz. La tercera demostración usa herramientas combinatorias y la cuarta está basada en resultados de Álgebra Lineal [1], los cuales se usan en el capítulo 3.

En el segundo capitulo verificamos que la conjetura es verdadera para algunos casos particulares, usando la función $s(n,2)$ definida por:

$$s(n,2) := \text{mín}\{|\mathcal{P}| : \mathcal{P} \subset \mathbb{Z} \times \mathbb{Z} \text{ y } \mathcal{P} \text{ tiene suma cero}\}.$$

Con base en el texto [29] realizamos el estudio de los casos $n = 2$ y $n = 3$ y reconstruimos en más detalle el caso $n = 3$. Para el estudio del caso $n = 5$ tomamos como referencia [24], verificamos los cálculos y de manera similar realizamos todos los cálculos para el caso $n = 7$ puesto que no aparecen en la literatura estudiada, donde se calculó las diferentes formas de la primera fila de los s-esquemas que pueden ocurrir y la tabla de la función $A_7(s,t)$ y con estos datos comprobamos que si se cumple la conjetura para $n = 7$.

En el tercer capítulo estudiamos las herramientas fundamentales para la demostración de algunas cotas muy cercanas al valor exacto de la función $s(n,2)$,

entre esas herramientas tenemos ingeniosos métodos algebraicos relacionados con el permanente de una matriz, polinomios no nulos con coeficientes en un campo finito [1] y la relación entre los monomios multilineales y las funciones definidas de $\{0,1\}^m$ en un campo [38]. Además, presentamos la prueba en detalle de un lema conocido como el Lema de Alon y Dubiner [1] el cual es consecuencia del Teorema de Chevalley-Warning [29]. Las cotas estimadas para la función $s(n,2)$ que estudiamos son dos: la estimada por N. Alon y M. Dubiner [1] en el año de 1993, ellos probaron que $s(n,2) \leq 6n-5$, aunque reducen el caso para $n=p$ primo ya que esta cota también es multiplicativa y la estudiamos puesto que es la primera cota superior estimada para dicha función; también estudiamos la cota estimada por L. Rónyai [38] quien se aproxima mucho al valor de la función pues prueba que $s(p,2) \leq 4p-2$, para p primo, implicando así que $s(p,2)$ o bien es $4p-3$ o $4p-2$. Aunque existe otra cota importante en este trabajo no la mencionamos, es la dada por W. Gao [18], prueba que la cota estimada por L. Rónyai se puede extender a potencias de primos, así $s(p^h,2) = 4p^h - 2$.

En el cuarto capítulo presentamos una reconstrucción de la prueba de la Conjetura de Kemnitz, con base en la referencia [37]; el aporte que hacemos en este trabajo es la ampliación, verificación y descripción en detalle de cada demostración de los resultados dados por el autor C. Rehier; en la primera sección se presentan cinco corolarios que tratan de algunas congruencias lineales que relacionan el número de subsecuencias de suma cero de una secuencia dada; como la herramienta principal que se utiliza para la prueba de estos corolarios es el Teorema de Chevalley-Warning, en algunos de ellos construimos los polinomios adecuados para la prueba de los mismos, que no aparecen reportados en la literatura; en la segunda sección se presenta primero un lema conocido como el Lema de Reiher [37] el cual es la base de la demostración de la conjetura la cual se prueba por contradicción. Lo curioso de esta prueba es el ingenio que tiene el autor para establecer esas relaciones de congruencias lineales que lo llevan a la demostración de la conjetura.

Los problemas de suma cero es un tema de frontera en la investigación actual ya que a partir de ellos surge la Teoría de Suma Cero; en la Teoría de Números Combinatoria los problemas de suma cero, los conjuntos suma y los cubrimientos de los enteros son tres diferentes tópicos iniciados por P. Erdös e investigados por muchos autores; éstos juegan un papel importante en la Teoría de Números y Combinatoria, existe una conexión profunda de estas tres áreas aparentemente no relacionadas y tienen por objeto establecer una teoría unificada, además tiene aplicaciones en muchos aspectos de campos finitos y Teoría de Grafos [46]. También los problemas de suma cero tienen relación con la Teoría de Ramsey [8] en el estudio sobre los números Ramsey de suma cero y con la Teoría de Códigos [34].

CAPÍTULO 1

EL TEOREMA DE ERDÖS, GINZBURG Y ZIV

A lo largo de este trabajo entenderemos por secuencia a una colección de elementos, no necesariamente todos distintos, de cierto conjunto dado, la denotaremos con doble llave, así: $\{\{\ \}\}$ y también entenderemos que un conjunto o una secuencia de $\mathbb{Z}_n$ tiene suma cero si la suma de todos sus elementos es congruente con cero módulo n, en caso contrario, diremos que el conjunto o la secuencia es libre de suma cero.

El Teorema de Erdös, Ginzburg y Ziv [14], originalmente se enuncia para números enteros, sin embargo podemos trabajar con secuencias en el grupo aditivo $\mathbb{Z}_n$ como se enuncia a continuación.

Teorema 1.1. *Para cualquier secuencia* $\{\{a_1, a_2, \ldots, a_{2n-1}\}\}$ *de elementos del grupo cíclico* $\mathbb{Z}_n$ *existe un conjunto* $I \subset \{1, 2, \ldots, 2n-1\}$ *de cardinalidad* n *tal que* $\sum_{i \in I} a_i = 0$ *(en* $\mathbb{Z}_n$*).*

De acuerdo a la demostración dada por Erdös, Ginzburg y Ziv [14], la prueba del Teorema 2.1 se reduce al caso cuando n es primo. Veamos que en efecto esto se cumple.

Sea $\{\{a_1, a_2, \ldots, a_{2n-1}\}\}$ una secuencia de elementos en $\mathbb{Z}_n$ de tamaño $2n-1$, supongamos que n es compuesto, digamos $n = uv$, donde $1 < u \leq v < n$ y además supongamos que el resultado se tiene para u y v.

De la secuencia dada $\{\{a_1, a_2, \ldots, a_{2n-1}\}\}$ escogemos $2v-1$ elementos, entre ellos existen v elementos, digamos $a_1, \ldots, a_v$ tales que

$$b_1 = \sum_{i=1}^{v} a_i \equiv 0 \, (mod \ v).$$

Luego, existen $(2n-1)-v = 2uv-1-v = (2u-1)v-1$ elementos en la secuencia original que no pertenecen a esta subsecuencia.

Ahora bien, entre los $(2u-1)v-1$ elementos restantes de la secuencia escogemos $2v-1$ elementos, entre ellos existen v elementos, digamos $a_{v+1}, \ldots, a_{2v}$ tales que

$$b_2 = \sum_{i=1}^{v} a_{v+i} \equiv 0 \, (\text{ mod } v).$$

Luego, existen $(2u-1)v-1-v = (2u-2)v-1$ elementos en la secuencia original que no pertenecen a las dos subsecuencias anteriores.

Continuando con el procedimiento, después de hacer $(2u-2)$ pasos, nos quedan $[2u-(2u-2)]v-1 = 2v-1$ elementos en la secuencia original que no pertenecen a las subsecuencias anteriores, entre estos elementos existen v, digamos

$$a_{(2u-2)v+1}, \ldots, a_{(2u-2)v+v},$$

tales que

$$b_{2u-1} = \sum_{i=1}^{v} a_{(2u-2)v+i} \equiv 0 \, (mod \ v).$$

Ahora tenemos $2u-1$ elementos, $b_1, \ldots, b_{2u-1}$, cada uno de los cuales es congruente con 0 módulo v. Como el resultado también es válido para u entonces entre los anteriores elementos existen u de ellos tales que

$$c = \sum_{j=1}^{u} b_j \equiv 0 \, (mod \ u),$$

o lo que es equivalente a

$$c = \sum_{i=1}^{uv} a_i \equiv 0 \, (mod \ uv).$$

Por lo tanto existen $uv = n$ elementos de $\{\{a_1, a_2, \ldots, a_{2n-1}\}\}$ cuya suma es congruente con cero módulo n.

1.1. Teorema de Cauchy-Davenport

El Teorema de Cauchy-Davenport [29] nos permite estimar un límite inferior para la cardinalidad del conjunto suma de dos subconjuntos de un grupo, a partir de las cardinalidades de los mismos. Este teorema fue probado en 1813 por Augustin Cauchy [7] y después en 1935 por Harold Davenport [11], quien no tenia conocimiento de la demostración de Cauchy.

Recordemos la definición de conjunto suma:

Definición 1.1. Sea $(G, +)$ un grupo abeliano. Si A, B son subconjuntos de G entonces su conjunto suma, denotado $A + B$, se define como:

$$A + B := \{a + b : a \in A, b \in B\}. \tag{1.1}$$

En esta sección presentamos la demostración del Teorema de Cauchy-Davenport haciendo uso de una técnica de la Teoría de Números Aditiva llamada la Transformada de Dyson como en [29], la cual fue desarrollada por Freeman Dyson, como parte de su prueba del Teorema de Mann [21] y fue utilizada por Olivier Ramaré en su trabajo sobre la Conjetura de Goldbach donde demostró que cada entero es la suma de a lo más seis primos [35].

Definición 1.2. Sea G un grupo abeliano. Sean $g \in G$ y A, B subconjuntos no vacíos de G. La Transformada de Dyson del par ordenado (A, B) respecto a g es el par (A_g, B_g) donde:

$$A_g = A \cup (B + g), \tag{1.2}$$

$$B_g = (A - g) \cap B. \tag{1.3}$$

La Transformada de Dyson [29] satisface las siguientes propiedades.

Proposición 1.1. *Sean A, B subconjuntos no vacíos de un grupo abeliano G y sea $g \in G$. Si (A_g, B_g) es la Transformada de Dyson del par (A, B) respecto a g entonces*

1. $A_g + B_g \subseteq A + B$,
2. $A_g \setminus A = g + (B \setminus B_g)$,
3. *Si A, B son conjuntos finitos entonces* $|A_g| + |B_g| = |A| + |B|$,
4. *Si $g \in A$ y $0 \in B$ entonces $g \in A_g$ y $0 \in B_g$.*

Demostración.

1. Consideremos el conjunto $A_g + B_g = \{\tilde{a} + \tilde{b} : \tilde{a} \in A_g, \tilde{b} \in B_g\}$.

   Sea $x \in A_g + B_g$ entonces $x = \tilde{a} + \tilde{b}$, para algún $\tilde{a} \in A_g$ y algún $\tilde{b} \in B_g$.

   De aquí que,
   $$[\tilde{a} \in A \cup (B + g)] \wedge [\tilde{b} \in (A - g) \cap B].$$

   Entonces pueden suceder dos casos:

   (i) Si $\tilde{a} \in A$, como $\tilde{b} \in B_g = (A-g) \cap B$ entonces $\tilde{b} \in B$, luego $\tilde{a}+\tilde{b} \in A+B$.

   (ii) Si $\tilde{a} \in B + g$, significa que existe $b \in B$ tal que $\tilde{a} = b + g$.

   Y como $\tilde{b} \in B_g$ entonces $\tilde{b} \in A - g$; es decir, existe $a \in A$ tal que $\tilde{b} = a - g$.

   Luego, $\tilde{a} + \tilde{b} = (b + g) + (a - g) = a + b \in A + B$.

   En consecuencia, $x \in A + B$ y así, $A_g + B_g \subseteq A + B$.

2. Observemos que:
   $$\begin{aligned} A_g \smallsetminus A &= [A \cup (B + g)] \smallsetminus A \\ &= (B + g) \smallsetminus A \\ &= \{b + g : b \in B, b + g \notin A\} \\ &= g + \{b \in B : b \notin (A - g)\} \\ &= g + \{b \in B : b \notin B_g\} \\ &= g + (B \smallsetminus B_g). \end{aligned}$$

3. Es claro que $A \subseteq A_g$ y $B_g \subseteq B$ por definición. Como por hipótesis A y B son subconjuntos finitos tenemos que:
   $$\begin{aligned} |A_g| - |A| &= |A_g \smallsetminus A| \\ &= |g + (B \smallsetminus B_g)| \\ &= |B \smallsetminus B_g| \\ &= |B| - |B_g|. \end{aligned}$$

   Esto implica que $|A_g| + |B_g| = |A| + |B|$.

4. Si $g \in A$ entonces $g \in A_g$, además $0 \in A - g$, y como $0 \in B$ entonces $0 \in (A - g) \cap B = B_g$.

□

A continuación vamos a demostrar el Teorema de Cauchy-Davenport con base en la demostración presentada en [29].

Teorema 1.2. *(Cauchy-Davenport)*

Sea p un número primo y sean A, B subconjuntos no vacíos de $\mathbb{Z}_p$. Entonces

$$|A + B| \geq min(p, |A| + |B| - 1). \tag{1.4}$$

Demostración. Consideremos dos casos:

Caso 1. $|A| + |B| > p$.

Dado que $|\mathbb{Z}_p| = p$ entonces $A + B = \mathbb{Z}_p$. En efecto, como A y B son subconjuntos de $\mathbb{Z}_p$, también lo es su conjunto suma; esto es, $A + B \subseteq \mathbb{Z}_p$.

De otro lado, sea $g \in \mathbb{Z}_p$ y consideremos el conjunto

$$g - B = \{g - b : b \in B\},$$

el cual satisface $|g - B| = |B|$.

Como $A \cup (g - B) \subseteq \mathbb{Z}_p$, tenemos

$$\begin{aligned} p = |\mathbb{Z}_p| &\geq |A \cup (g - B)| \\ &\geq |A| + |g - B| - |A \cap (g - B)| \\ &= |A| + |B| - |A \cap (g - B)|. \end{aligned}$$

De esto se sigue que, $A \cap (g - B) \neq \emptyset$, pues si no fuese así $p \geq |A| + |B|$, contradiciendo la hipótesis. Así,

$$|A \cap (g - B)| \geq |A| + |B| - p > 0.$$

Luego, tomando $|A \cap (g - B)| \geq 1$, existe al menos un elemento $x \in A \cap (g - B)$; es decir, existen $a \in A$ y $b \in B$ tales que $x = a$ y $x = g - b$, de donde $g = a + b$.

Así, $g \in A + B$ y por lo tanto $\mathbb{Z}_p \subseteq A + B$.

En consecuencia, el teorema es válido para este caso.

Caso 2. $|A| + |B| \leq p$

Como mín$\{p, |A| + |B| - 1\} = |A| + |B| - 1$ es suficiente probar que

$$|A + B| \geq |A| + |B| - 1.$$

Para ello aplicamos inducción sobre $|B|$.

Sin pérdida de generalidad, supongamos que $0 \in B$, pues de lo contrario consideramos el conjunto $B - b = \hat{B}$, para algún $b \in B$, y aplicamos inducción a $|\hat{B}|$.

Si $|B| = 1$ entonces $B = \{0\}$ y así $A + B = A$, luego $|A + B| = |A| = |A| + |B| - 1$ y por lo tanto el teorema se cumple para este caso.

Supongamos que $|B| \geq 2$ y que el teorema es válido para todo subconjunto propio de B.

Afirmamos que $A \neq A + B$. En efecto, escojamos $b \in B \setminus \{0\}$, fijemos $a \in A$ y consideremos los elementos $a, a + b, \ldots, a + kb$, para cada k entero.

Si suponemos que $A = A + B$ entonces los elementos $a, a + b, \ldots, a + kb$ deben estar en A. Como esto se cumple para cada k, en particular se cumple para $k = p$ pero todos los elementos son distintos; en efecto, supongamos que existen dos elementos iguales $a + ib = a + jb$, con $i \neq j$ entonces $(i - j)b = 0$ y como $b \neq 0$ implica que $i = j$, contradicción, y como $|A| = p$ entonces $A = \mathbb{Z}_p$, lo cual no puede ser posible ya que $|A| + |B| \leq p$ y $|B| \geq 2$.

Por otro lado, para $a \in A$ consideremos la Transformada de Dyson del par (A, B) respecto a a, donde

$$A_a = A \cup (B + a),$$
$$B_a = (A - a) \cap B.$$

Dado que $B_a \subseteq B$ tenemos que $|B_a| \leq |B|$. Veamos que la desigualdad es estricta.

Supongamos que $|B_a| = |B|$ para cada $a \in A$ entonces $B \subseteq A - a$ y así, $B + a \subseteq A$, para todo $a \in A$.

Por tanto, $A + B \subseteq A$ y como $0 \in B$ entonces $A \subseteq A + B$; de esta manera, $A + B = A$ contradiciendo lo demostrado anteriormente. Por consiguiente, tenemos que $|B_a| < |B|$; es decir, B_a es un subconjunto propio de B.

Ahora bien, por las propiedades de la Transformada de Dyson tenemos:

$$|A_a| + |B_a| = |A| + |B| \leq p$$

y aplicando la hipótesis inductiva al conjunto B_a obtenemos que

$$|A_a + B_a| \geq |A_a| + |B_a| - 1.$$

Luego por la propiedad (1) de la Proposición 1.1 tenemos:

$$\begin{aligned} |A + B| &\geq |A_a + B_a| \\ &\geq |A_a| + |B_a| - 1 \\ &= |A| + |B| - 1. \end{aligned}$$

En consecuencia, el teorema es válido para este caso. □

Ahora, si tenemos h subconjuntos no vacíos de $\mathbb{Z}_p$ nos podemos preguntar si el Teorema de Cauchy- Davenport también es válido. La respuesta es afirmativa, el teorema que sigue es una generalización del Teorema de Cauchy- Davenport [29].

Teorema 1.3. *Sean $h \geq 2$, p un número primo y $A_1, \ldots, A_h$ subconjuntos no vacíos de $\mathbb{Z}_p$. Entonces*

$$|A_1 + \cdots + A_h| \geq \text{mín}\left(p, \sum_{i=1}^{h} |A_i| - h + 1\right). \tag{1.5}$$

Demostración. Apliquemos inducción sobre h.

Si $h = 2$, es el Teorema de Cauchy-Davenport.

Supongamos que se cumple para $h - 1$ subconjuntos de $\mathbb{Z}_p$.

Sean $A_1, \ldots, A_h$ subconjuntos no vacíos de $\mathbb{Z}_p$ y consideremos el conjunto

$$B = A_1 + \cdots + A_{h-1}.$$

Por la hipótesis inductiva tenemos que:

$$\begin{aligned} |B| &= |A_1 + \cdots + A_{h-1}| \\ &\geq \text{mín}(p, \sum_{i=1}^{h-1} |A_i| - (h-1) + 1) \\ &= \text{mín}(p, \sum_{i=1}^{h-1} |A_i| - h + 2). \end{aligned}$$

Así,

$$\begin{aligned} |A_1 + \cdots + A_h| &= |(A_1 + \cdots + A_{h-1}) + A_h| \\ &= |B + A_h| \\ &\geq \text{mín}(p, |B| + |A_h| - 1) \\ &\geq \text{mín}(p, (\sum_{i=1}^{h-1} |A_i| - h + 2) + |A_h| - 1) \\ &= \text{mín}(p, \sum_{i=1}^{h} |A_i| - h + 1). \end{aligned}$$

Esto completa la demostración. □

1.2. Teorema de Chevalley-Warning

Ahora vamos a estudiar el Teorema de Chevalley-Warning [29], el cual trata sobre el número de soluciones de sistemas de ecuaciones sobre un campo finito. Este teorema fue conjeturado por Emil Artin en 1934, demostrado primero por Claude Chevalley [9] en el año de 1935 y extendido por Ewald Warning [43] en el mismo año.

En este trabajo el Teorema de Chevalley-Warning será usado para demostrar el Teorema de Erdös, Ginzburg y Ziv y la Conjetura de Kemnitz siendo en este último el argumento principal de las demostraciones.

Para la demostración del Teorema de Chevalley-Warning usaremos el siguiente resultado de Teoría de Campos Finitos.

Lema 1.1. *Sea p un número primo y sea $\mathbb{F}_q$ un campo finito con $q = p^t$ elementos, donde t es un entero positivo, entonces para todo $0 \leq r < q - 1$, se cumple*

$$\sum_{x \in \mathbb{F}_q} x^r = 0. \tag{1.6}$$

Demostración. Para $r = 0$, si adoptamos la convención que $0^0 = 1$, tenemos que:

$$\sum_{x \in \mathbb{F}_q} x^0 = \sum_{x \in \mathbb{F}_q} 1 = q \equiv 0 \, (mod \ p).$$

Para $0 < r < q-1$ tenemos que:

$$\sum_{x\in\mathbb{F}_q} x^r = 0^r + \sum_{x\in\mathbb{F}_q^*} x^r = \sum_{x\in\mathbb{F}_q^*} x^r.$$

Como el grupo multiplicativo $\mathbb{F}_q^*$ de elementos no nulos de un campo finito es cíclico entonces $\mathbb{F}_q^* = \langle\theta\rangle = \{\theta, \theta^2, \ldots, \theta^{(q-1)}\}$. Así los elementos de $\mathbb{F}_q^*$ son potencias de θ.

Ahora bien, llamemos $\theta^r = \beta \neq 1$, luego

$$\begin{aligned}
\sum_{x\in\mathbb{F}_q^*} x^r &= \sum_{i=1}^{q-1} (\theta^i)^r \\
&= \sum_{i=1}^{q-1} \theta^{ir} \\
&= \theta^r + \theta^{2r} + \cdots + \theta^{(q-1)r} \\
&= \theta^r(1 + \theta^r + \cdots + \theta^{(q-2)r}) \\
&= \beta(1 + \beta + \cdots + \beta^{q-2}) \\
&= \beta(\tfrac{\beta^{q-1}-1}{\beta-1}) \\
&= \beta(\tfrac{1-1}{\beta-1}) \\
&= 0.
\end{aligned}$$

Esto completa la demostración. □

Ahora vamos a probar el Teorema de Chevalley-Warning con base en [29].

Teorema 1.4. *(Chevalley-Warning)*

Sean p un número primo y $\mathbb{F}_q$ el campo finito con $q = p^t$ elementos, donde t es un entero positivo. Para $i = 1, \ldots, m$, sean $P_i(x_1, \ldots, x_n)$ polinomios de grado d_i en n variables con coeficientes en $\mathbb{F}_q$.

Si $\sum_{i=1}^{m} d_i < n$ entonces el número N de ceros comunes de $P_1, \ldots, P_m$ (en $\mathbb{F}_q^n$) satisface

$$N \equiv 0 \,(\text{mod } p). \tag{1.7}$$

En particular, si existe un cero común entonces existe otro.

Demostración. Como el grupo multiplicativo de elementos no nulos de un campo finito es cíclico, para cualquier $x \in \mathbb{F}_q$, tenemos que

$$x^{q-1} = \begin{cases} 1 & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \tag{1.8}$$

Tomemos $x_1, \ldots, x_n$ en $\mathbb{F}_q$, entonces $P_i(x_1, \ldots, x_n) \in \mathbb{F}_q$, para todo $i = 1, \ldots, m$ y por (1.8), tenemos:

$$P_i(x_1, \ldots, x_n)^{q-1} = \begin{cases} 1 & \text{si } P_i(x_1, \ldots, x_n) \neq 0 \\ 0 & \text{si } P_i(x_1, \ldots, x_n) = 0 \end{cases} \tag{1.9}$$

Ahora consideremos el siguiente producto:

$$\prod_{i=1}^{m}(1 - P_i(x_1, \ldots, x_n)^{q-1}) = \begin{cases} 1 & \text{si } P_i(x_1, \ldots, x_n) = 0 \\ 0 & \text{en otro caso} \end{cases} \tag{1.10}$$

Así, el número de ceros comunes de los polinomios $P_1, \ldots, P_m$ en $\mathbb{F}_q^n$ es:

$$N = \sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \prod_{i=1}^{m}(1 - P_i(x_1, \ldots, x_n)^{q-1}). \tag{1.11}$$

Dado que el grado de P_i es d_i, para cada $i = 1, \ldots, m$, se sigue que:

$$\prod_{i=1}^{m}(1 - P_i(x_1, \ldots, x_n)^{q-1}) = \sum_{(r_1,\ldots,r_n)} a_{r_1,\ldots,r_n} x_1^{r_1} \ldots x_n^{r_n} \tag{1.12}$$

es un polinomio de grado a lo más $(q-1)\sum_{i=1}^{m} d_i$ con coeficientes $a_{r_1,\ldots,r_n} \in \mathbb{F}_q$. Es decir, la sumatoria del lado derecho recorre sobre todas las n-uplas $(r_1, \ldots, r_n)$ de enteros no negativos tales que:

$$\sum_{j=1}^{n} r_j \leq (q-1)\sum_{i=1}^{m} d_i. \tag{1.13}$$

Entonces

$$\begin{aligned} N &\equiv \sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \prod_{i=1}^{m}(1 - P_i(x_1, \ldots, x_n)^{q-1}) \,(mod\ p) \\ &\equiv \sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \sum_{(r_1,\ldots,r_n)} a_{r_1,\ldots,r_n} x_1^{r_1} \ldots x_n^{r_n} \,(mod\ \mathrm{p}) \\ &\equiv \sum_{(r_1,\ldots,r_n)} \sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} a_{r_1,\ldots,r_n} x_1^{r_1} \ldots x_n^{r_n} \,(mod\ p) \\ &\equiv \sum_{(r_1,\ldots,r_n)} a_{r_1,\ldots,r_n} \sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} x_1^{r_1} \ldots x_n^{r_n} \,(mod\ p) \\ &\equiv \sum_{(r_1,\ldots,r_n)} a_{r_1,\ldots,r_n} \prod_{j=1}^{n} \sum_{x_j\in\mathbb{F}_q} x_j^{r_j} \,(mod\ p). \end{aligned}$$

Como por hipótesis, $\sum_{i=1}^{m} d_i < n$, y por (1.13) tenemos que $\sum_{j=1}^{n} r_j \leq (q-1)\,n$, esto implica que existe $j \in \{1, \ldots, n\}$, tal que $0 \leq r_j < q-1$. Así, por el Lema 1.1 obtenemos:

$$\sum_{x_j \in \mathbb{F}_q} x_j^{r_j} \equiv 0\,(mod\ p),$$

y por consiguiente,

$$\prod_{j=1}^{n} \sum_{x_j \in \mathbb{F}_q} x_j^{r_j} \equiv 0\,(mod\ p).$$

En conclusión, $N \equiv 0\,(mod\ p)$. □

1.3. Teorema de Lucas

Cuando usamos números muy grandes y difíciles de expresar, podemos estudiar sus propiedades sin necesidad de hallar explícitamente dichos números; por ejemplo, los coeficientes binomiales crecen rápidamente a medida que los números se van haciendo mayores, ya que están involucrados los factoriales, el teorema que sigue a continuación nos permite estudiar las propiedades de dichos números y se conoce como el Teorema de Lucas, el cual nos da un algoritmo sencillo para encontrar el resto de dividir cualquier coeficiente binomial entre un número primo p.

Este teorema lo usaremos para la prueba de algunos coeficientes binomiales en particular, utilizados en la demostración del Teorema de Erdös, Ginzburg y Ziv en la siguiente sección cuando presentamos la Demostración 3. de dicho teorema. Además, es usado en la prueba de la cota estimada por Lajos Rónyai [38] y en la prueba del Corolario 4.6.

Para la demostración del Teorema de Lucas vamos a tener en cuenta la siguiente observación.

Una de las aplicaciones de mayor utilidad que ofrece el algoritmo de la división de Euclides, es la representación de cualquier número natural mediante combinación lineal de potencias de un número primo p. Esto es, dado b un número entero positivo, existen enteros únicos $r_0, r_1, \ldots, r_n$ tales que:

$$b = r_n p^n + r_{n-1} p^{n-1} + \cdots + r_1 p + r_0, \tag{1.14}$$

con $0 \leq r_i \leq p-1$, para todo $i = 0, \ldots, n$.

Teorema 1.5. *(Teorema de Lucas)*

Sean m, n números enteros no negativos con $m > n$, p un número primo y sean

$$m = m_k p^k + \cdots + m_1 p + m_0, \tag{1.15}$$

$$n = n_k p^k + \cdots + n_1 p + n_0, \tag{1.16}$$

lo desarrollos de m y n en base p, respectivamente.

Entonces

$$\left(\begin{array}{c} m \\ n \end{array} \right) \equiv \prod_{i=0}^{k} \left(\begin{array}{c} m_i \\ n_i \end{array} \right) (\text{mod } p). \tag{1.17}$$

En particular, el coeficiente binomial $\left(\begin{array}{c} m \\ n \end{array} \right)$ es divisible por un número p tan pronto como al menos uno de los dígitos de n en base p es mayor que el dígito correspondiente de m.

Demostración. Trabajemos con polinomios en la variable x y coeficientes en $\mathbb{Z}_p$.

Por el teorema del binomio tenemos que:

$$(1+x)^p = \sum_{i=0}^{p} \left(\begin{array}{c} p \\ i \end{array} \right) x^i \equiv 1 + x^p (mod\ p), \tag{1.18}$$

pues $\left(\begin{array}{c} p \\ i \end{array} \right) \equiv 0\,(mod\ p),$ para todo $1 \leq i \leq p-1$.

Más generalmente, tenemos que $(1+x)^{p^i} \equiv 1 + x^{p^i} (mod\ p)$, cuya demostración se hace por inducción.

Dado que $m = m_k p^k + \cdots + m_1 p + m_0$, tenemos que el polinomio se puede escribir

de la siguiente manera:

$$\begin{aligned}(1+x)^m &= (1+x)^{\left(\sum_{i=0}^{k} m_i p^i\right)} \\ &= \prod_{i=0}^{k}(1+x)^{m_i p^i} \\ &= \prod_{i=0}^{k}[(1+x)^{p^i}]^{m_i} \\ &\equiv \prod_{i=0}^{k}(1+x^{p^i})^{m_i}(mod\ p) \\ &\equiv \prod_{i=0}^{k}\sum_{j=0}^{m_i}\left(\begin{array}{c} m_i \\ j \end{array}\right) x^{jp^i}(mod\ p).\end{aligned}$$

De otro lado, como $(1+x)^m = \sum_{i=0}^{m}\left(\begin{array}{c} m \\ i \end{array}\right) x^i$, la anterior expresión nos queda así:

$$\sum_{i=0}^{m}\left(\begin{array}{c} m \\ i \end{array}\right) x^i \equiv \prod_{i=0}^{k}\sum_{j=0}^{m_i}\left(\begin{array}{c} m_i \\ j \end{array}\right) x^{jp^i}(mod\ p). \tag{1.19}$$

Luego el coeficiente de x^n en (1.19) es $\left(\begin{array}{c} m \\ n \end{array}\right)$ para el lado izquierdo y para el lado derecho es $\prod_{i=0}^{k}\left(\begin{array}{c} m_i \\ n_i \end{array}\right)$.

Así, igualando los coeficientes de x^n se obtiene el resultado deseado. □

Usando el Teorema de Lucas obtenemos el siguiente resultado, tomado de Zhi-Wei Sun [44].

Teorema 1.6. *Sea $n = p^h$ donde p es un número primo y h es un entero no negativo. Entonces*

$$\left(\begin{array}{c} 2n-1 \\ n \end{array}\right) \equiv 1 \,(\text{mod } p) \tag{1.20}$$

y

$$\left(\begin{array}{c} 2n-1-k \\ n-1 \end{array}\right) \equiv 0 \,(\text{mod } p), \tag{1.21}$$

para $k = 1, \ldots, n-1$.

Demostración. Si $h = 0$ el teorema es trivial, de esta manera supongamos que $h \geq 1$.

Sea $k \in \{0, 1, \ldots, n-1\}$ y como $0 \leq n-1-k < n = p^h$, podemos escribir $n-1-k$ como combinación lineal de potencias de p así,

$$n - 1 - k = \sum_{i=0}^{h-1} k_i p^i, \tag{1.22}$$

donde $k_i \in \{0, 1, \ldots, p-1\}$.

De aquí que,

$$\begin{pmatrix} 2n-1-k \\ n-1 \end{pmatrix} = \begin{pmatrix} 1p^h + k_{h-1}p^{h-1} + \cdots + k_0 p^0 \\ 0p^h + (p-1)p^{h-1} + \cdots + (p-1)p^0 \end{pmatrix}. \tag{1.23}$$

Por el Teorema 2.5 tenemos que:

$$\begin{pmatrix} 2n-1-k \\ n-1 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} k_{h-1} \\ p-1 \end{pmatrix} \cdots \begin{pmatrix} k_0 \\ p-1 \end{pmatrix} (mod\ p). \tag{1.24}$$

Si $k = 0$ entonces $k_0 = \cdots = k_{h-1} = p-1$ y por lo tanto reemplazando en (1.24) obtenemos

$$\begin{pmatrix} 2n-1 \\ n \end{pmatrix} = \begin{pmatrix} 2n-1 \\ n-1 \end{pmatrix} \equiv 1\,(mod\ p). \tag{1.25}$$

De otro lado, cuando $0 < k < n$, claramente $k_i < p-1$ para algún $0 \leq i \leq h-1$ y por lo tanto reemplazando en (1.24) tenemos que:

$$\begin{pmatrix} 2n-1-k \\ n-1 \end{pmatrix} \equiv 0(mod\ p). \tag{1.26}$$

□

1.4. Permanente de una matriz

En matemáticas, el cálculo del permanente de una matriz es un problema más complejo que el cálculo del determinante a pesar de la aparente similitud de las definiciones. El permanente se define de manera similar a los determinantes, como una suma de productos de juegos de entradas de la matriz que se encuentran en distintas filas y columnas. Sin embargo, cuando el factor determinante asigna un signo a cada uno de estos productos, el permanente no lo hace. Uno de los

métodos más eficaces para el cálculo de los permanentes es mediante la fórmula Ryser [39, 40].

El permanente es usado en Algebra lineal, Teoría de la Probabilidad y Combinatoria. En Combinatoria, el permanente se puede interpretar de la siguiente manera: el número de sistemas de distintos representantes para una determinada familia de subconjuntos de un conjunto finito es el permanente de una matriz de incidencia para el sistema de incidencia relacionado con esta familia [20].

Son de mucho interés el estudio del permanente de una matriz compuesta de ceros y unos, también de una matriz con entradas en los números reales no negativos, en particular, las matrices doblemente estocásticas (en los que la suma de los elementos de cualquier fila y cualquier columna es 1) [26], y de una matriz hermitiana compleja [27], entre otras.

En este trabajo usaremos algunas propiedades del permanente para la demostración del Teorema de Erdös, Ginzburg y Ziv y de la cota estimada por N. Alon y M. Dubiner [1].

Definición 1.3. (*Permanente*)

El ***permanente*** de una matriz A de tamaño $n \times n$ es

$$per(A) = \sum_{\sigma \in S_n} a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}, \tag{1.27}$$

donde S_n es el grupo simétrico de n elementos.

Ahora bien, consideremos los vectores $x = (x_1, x_2, \dots, x_n)^T$ e $y = (y_1, y_2, \dots, y_n)^T$ y la matriz $A = (a_{ij})$ de tamaño $n \times n$. Sea $y = Ax$ y definimos el polinomio en n variables por:

$$\begin{aligned} P(x_1, x_2, \dots, x_n) &= \prod_{i=1}^{n} y_i \\ &= (a_{11}x_1 + \dots + a_{1n}x_n) \cdot (a_{21}x_1 + \dots + a_{2n}x_n) \cdots \\ &\quad (a_{n1}x_1 + \dots + a_{nn}x_n) \\ &= \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij}x_j \right). \end{aligned} \tag{1.28}$$

Todos los términos del polinomio P son de grado n.

Si hacemos la expansión de (1.28) podemos observar que el coeficiente del término $x_1 \cdot x_2 \cdots x_n$ se puede obtener sumando sobre todas las permutaciones posibles de

S_n, así:

$$\sum_{\sigma\in S_n} a_{1\sigma(1)}x_{\sigma(1)}\cdot a_{2\sigma(2)}x_{\sigma(2)}\cdots a_{n\sigma(n)}x_{\sigma(n)} = \left(\sum_{\sigma\in S_n} a_{1\sigma(1)}a_{2\sigma(2)}\ldots a_{n\sigma(n)}\right) x_1\cdot x_2\cdots x_n.$$

De esta manera, el $per(A)$ es el coeficiente del término $x_1\cdot x_2\cdots x_n$ en el polinomio dado en (1.28). Esta definición la usaremos más adelante en algunos lemas.

Por otro lado, al igual que en el determinante de una matriz, el permanente satisface la *expansión de Laplace*; esto es, supongamos que A es una matriz $n\times n$ y A_{ij} es la submatriz de A que se obtiene al eliminar la i-ésima fila y la j-ésima columna. Entonces para $i = 1,\ldots,n$

$$per(A) = \sum_{j=1}^{n} a_{ij}per(A_{ij}). \tag{1.29}$$

La siguiente propiedad que cumple el permanente de una matriz en particular será usada en la Demostración 4. del Teorema de Erdös, Ginzburg y Ziv, me pareció importante presentarla como una proposición y hacer la demostración pues en el artículo [1] únicamente se usa este resultado.

Proposición 1.2. *Dada la matriz de la forma*

$$A = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1 & a_2 & \ldots & a_n \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \ldots & a_n \end{pmatrix},$$

se cumple que:

$$per(A) = n!\, a_1a_2\ldots a_n. \tag{1.30}$$

Demostración. Probemos esto por inducción sobre n.

Para $n = 2$, tenemos

$$A = \begin{pmatrix} a_1 & a_2 \\ a_1 & a_2 \end{pmatrix}.$$

Luego, $per(A) = a_1a_2 + a_2a_1 = 2a_1a_2 = 2!\, a_1a_2$.

Supongamos que el enunciado se cumple para $n-1$; esto es, para la matriz

$$A = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n-1} \\ a_1 & a_2 & \ldots & a_{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \ldots & a_{n-1} \end{pmatrix},$$

se cumple que $per(A) = (n-1)!\, a_1 a_2 \dots a_{n-1}$.

Ahora, verifiquemos que el enunciado es verdadero para n.

Sea la matriz

$$B = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \dots & a_n \end{pmatrix},$$

calculemos el permanente de B usando la expansión de Laplace, así:

$$per(B) = a_1 per(B_1) + a_2 per(B_2) + \cdots + a_n per(B_n), \tag{1.31}$$

donde para todo $i = 1, \dots, n$ la matriz

$$B_i = \begin{pmatrix} a_1 & a_2 & \dots & a_{i-1} & a_{i+1} & \dots & a_n \\ a_1 & a_2 & \dots & a_{i-1} & a_{i+1} & \dots & a_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \dots & a_{i-1} & a_{i+1} & \dots & a_n \end{pmatrix}.$$

Como las matrices B_i son de tamaño $(n-1) \times (n-1)$, para cada $i = 1, \dots, n$, por la hipótesis inductiva tenemos:

$$\begin{aligned} per(B) &= a_1[(n-1)! a_2 a_3 \dots a_n] + a_2[(n-1)! a_1 a_3 \dots a_n] + \cdots \\ &\quad + a_n[(n-1)! a_1 a_2 \dots a_{n-1}] \\ &= n! a_1 a_2 \dots a_n. \end{aligned}$$

Luego, el enunciado es válido para todo $n \in \mathbb{N}$. □

De otro lado, recordemos que el número de subconjuntos $U \neq \emptyset$ del conjunto $\{1, \dots, m\}$ es $2^m - 1$ y este número es equivalente al número de subconjuntos que contienen al elemento m más el número de subconjuntos que no lo contienen; esto es, $2^{m-1} + (2^{m-1} - 1)$.

Esta observación nos ayuda para la prueba del siguiente lema presentado en [3].

Además, llamemos $r = 2^m - 1, s = 2^{m-1}, t = 2^{m-1} - 1$, así $s + t = r$ y supongamos que los subconjuntos $U \subseteq \{1, \dots, m\}$ que contienen al elemento m son $U_1, \dots, U_s$ y los que no lo contienen son $U_{s+1}, \dots, U_r$

Lema 1.2. *Sea*

$$P = P(x_1, \ldots, x_m) = \sum_{U \subseteq \{1,\ldots,m\}} b_U \cdot \prod_{i \in U} x_i \tag{1.32}$$

un polinomio multilineal sobre un anillo conmutativo con identidad.

Si $P(y_1, \ldots, y_m) = 0$ *para cada* $(y_1, \ldots, y_m)$ *en* $\{0,1\}^m$ *entonces* $P \equiv 0$*; esto es,* $b_U = 0$ *para todo* $U \subseteq \{1, \ldots, m\}$.

Demostración. Apliquemos inducción sobre m.

Para $m = 1$ el resultado es trivial. Supongamos que el resultado es válido para $m-1$; es decir, si $\widetilde{P}(y_1, \ldots, y_{m-1}) = 0$ para cada $(y_1, \ldots, y_{m-1})$ en $\{0,1\}^{m-1}$ entonces $\widetilde{P} \equiv 0$.

Ahora, verifiquemos que el enunciado se cumple para m.

Dado un polinomio, como en (1.32),

$$P = P(x_1, \ldots, x_m) = \sum_{U \subseteq \{1,\ldots,m\}} b_U \cdot \prod_{i \in U} x_i \,,$$

lo podemos escribir de la siguiente manera:

$$\begin{aligned} P(x_1, \ldots, x_m) \; &= b_{U_1} \cdot \textstyle\prod_{i \in U_1} x_i + \cdots + b_{U_s} \cdot \prod_{i \in U_s} x_i \; + \\ &\quad b_{U_{s+1}} \cdot \textstyle\prod_{i \in U_{s+1}} x_i + \cdots + b_{U_r} \cdot \prod_{i \in U_r} x_i, \\ &= \Big(b_{U_1} \cdot \textstyle\prod_{i \in U_1 \setminus \{m\}} x_i + \cdots + b_{U_s} \cdot \prod_{i \in U_s \setminus \{m\}} x_i \Big) x_m \; + \\ &\quad b_{U_{s+1}} \cdot \textstyle\prod_{i \in U_{s+1}} x_i + \cdots + b_{U_r} \cdot \prod_{i \in U_r} x_i, \\ &= P_1(x_1, \ldots, x_{m-1}) x_m + P_2(x_1, \ldots, x_{m-1}), \end{aligned}$$

donde P_1 y P_2 son polinomios multilineales en las variables $x_1, \ldots, x_{m-1}$.

Como por hipótesis $P(y_1, \ldots, y_m) = P_1(y_1, \ldots, y_{m-1}) y_m + P_2(y_1, \ldots, y_{m-1}) = 0$, para cada $(y_1, \ldots, y_m)$ en $\{0,1\}^m$ debemos probar que $P_i(y_1, \ldots, y_{m-1}) = 0$, para $i = 1, 2$ y cada $(y_1, \ldots, y_{m-1})$ en $\{0,1\}^{m-1}$.

En efecto, fijemos la $(m-1)$- tupla $(y_1, \ldots, y_{m-1})$ en $\{0,1\}^{m-1}$ y consideremos el polinomio:

$$Q(x_m) = P(y_1, \ldots, y_{m-1}, x_m) = P_1(y_1, \ldots, y_{m-1}) x_m + P_2(y_1, \ldots, y_{m-1}),$$

el cual tiene grado a lo más 1 y es tal que:

$$Q(y_m) = P(y_1, \ldots, y_{m-1}, y_m) = 0,$$

para todo $y_m \in \{0,1\}$.

Como $Q(x_m)$ tiene a lo más una raíz y $|\{0,1\}| = 2$, entonces $Q(x_m)$ es el polinomio nulo, así

$$P_i(y_1, \ldots, y_{m-1}) = 0,$$

para $i = 1, 2$ y cada $(y_1, \ldots, y_{m-1}) \in \{0,1\}^{m-1}$.

Ahora, como los polinomios P_1 y P_2 satisfacen las hipótesis del lema, por la hipótesis inductiva tenemos que $P_1 \equiv P_2 \equiv 0$ y así, $P \equiv 0$. Completando la demostración. □

El siguiente lema dado en [1], muestra la conexión entre el permanente de una matriz y las posibles sumas de subconjuntos del conjunto de columnas de la matriz.

Lema 1.3. *Sea $A = (a_{ij})$ una matriz de tamaño $m \times m$ sobre $\mathbb{Z}_p$ y supongamos que $per(A) \neq 0$ en $\mathbb{Z}_p$. Entonces para cualquier $c = (c_1, \ldots, c_m)$ en $\mathbb{Z}_p^m$ existen $\epsilon_1, \ldots, \epsilon_m$ en $\{0,1\}$ tales que*

$$\sum_{j=1}^{m} \epsilon_j a_{ij} \neq c_i, \tag{1.33}$$

para todo $1 \leq i \leq m$. En otras palabras, para cualquier vector c existe un subconjunto de columnas de A cuya suma difiere de c en cada coordenada.

Demostración. Supongamos que el lema es falso y que no existen $\epsilon_1, \ldots, \epsilon_m$ como el enunciado. Dada la matriz $A = (a_{ij})$, consideremos el polinomio

$$P = P(x_1, \ldots, x_m) = \prod_{i=1}^{m} (\sum_{j=1}^{m} a_{ij} x_j - c_i), \tag{1.34}$$

donde $c_i \in \mathbb{Z}_p$.

Por suposición, para algún $c_i \in \mathbb{Z}_p$

$$\sum_{j=1}^{m} a_{ij} x_j = c_i, \tag{1.35}$$

y por lo tanto $P(x_1, \ldots, x_m) = 0$, para todo $(x_1, \ldots, x_m)$ en $\{0,1\}^m$.

Sea $\overline{P} = \overline{P}(x_1, \ldots, x_m)$ el polinomio multilineal que se obtiene de P, al escribir P como una suma de monomios y reemplazar por

$$a_U \prod_{i \in U} x_i, \tag{1.36}$$

a cada monomio de la forma $a_U \prod_{i \in U} x_i^{\delta_i}$ con $U \subseteq \{1, \ldots, m\}$ y $\delta_i > 0$.

Claramente $\overline{P}(x_1, \ldots, x_m) = P(x_1, \ldots, x_m) = 0$, para todo $(x_1, \ldots, x_m)$ en $\{0,1\}^m$. Por el Lema 1.2 tenemos que $\overline{P} \equiv 0$, pero esto es imposible pues el coeficiente del término $\prod_{i=1}^{m} x_i$ en $\overline{P}$, el cual es equivalente al coeficiente de este producto en P, es $per(A) \neq 0$. En consecuencia, la afirmación del lema se tiene.

□

1.5. Cuatro Demostraciones del Teorema de Erdös, Ginzburg y Ziv

Vamos a demostrar el Teorema de Erdös, Ginzburg y Ziv, con base en la referencia [1], usando las distintas herramientas que estudiamos en las secciones anteriores. Además, como ya mencionamos en un principio este teorema es suficiente probarlo para el caso de primos, por tal razón lo enunciamos de la siguiente manera:

Teorema 1.7. *(Erdös, Ginzburg y Ziv)*

Sea p un número primo. Para cualquier secuencia $\{\{a_1, a_2, \ldots, a_{2p-1}\}\}$ *de elementos del grupo cíclico* $\mathbb{Z}_p$*, existe un conjunto* $I \subset \{1, 2, \ldots, 2p-1\}$ *de cardinalidad p tal que*

$$\sum_{i \in I} a_i = 0. \tag{1.37}$$

Para la primera demostración que presentamos en detalle usando el Teorema de Cauchy-Davenport, tomamos como base el texto [29] (Capitulo 2).

Demostración 1. Sea $\{\{a_1, \ldots, a_{2p-1}\}\}$ una secuencia de elementos en el campo finito $\mathbb{Z}_p$. Renumeramos los elementos a_i de tal modo que:

$$0 \leq a_1 \leq \cdots \leq a_{2p-1} < p.$$

Podemos considerar dos casos:

(i) Si $a_i = a_{i+p-1}$ para algún $i \in \{1, \ldots, p\}$ entonces

$$a_i = a_{i+1} = \cdots = a_{i+p-1},$$

de aquí que

$$\begin{aligned} a_i &= a_i \\ a_{i+1} &= a_i \\ &\vdots \\ a_{i+p-1} &= a_i. \end{aligned}$$

Sumando cada lado obtenemos:

$$a_i + a_{i+1} + \cdots + a_{i+p-1} = pa_i = 0$$

Luego la subsecuencia buscada es $\{\{a_i, \ldots, a_{i+p-1}\}\}$, para algún $i = 1, \ldots, p$.

(ii) Si $a_i \neq a_{i+p-1}$ para todo $i \in \{1, \ldots, p\}$ entonces consideremos los siguientes conjuntos:

$$A_i = \{a_i, a_{i+p-1}\} \subseteq \mathbb{Z}_p,$$

los cuales satisfacen que $|A_i| = 2$ para $i \in \{1, \ldots, p-1\}$.

Aplicamos el Teorema 1.3 a estos conjuntos y obtenemos que:

$$|A_1 + \ldots + A_{p-1}| \geq \text{mín}(p, 2(p-1) - (p-1) + 1) = p,$$

luego,

$$A_1 + \cdots + A_{p-1} = \mathbb{Z}_p.$$

Por consiguiente, existen clases de congruencia $a_{j_i} \in A_i$ tales que cada $j_i \in \{i, i+p-1\}$, para $i = 1, \ldots, p-1$ y así,

$$-a_{2p-1} = a_{j_1} + \cdots + a_{j_{p-1}},$$

esto es:

$$a_{2p-1} + a_{j_1} + \cdots + a_{j_{p-1}} = 0.$$

Luego la subsecuencia buscada es $\{\{a_{2p-1}, a_{j_1}, \ldots, a_{j_{p-1}}\}\}$.

□

Al igual que la anterior demostración, para la segunda demostración presentada tomamos como base el texto [29] (Capítulo 2) en la cual se hace uso del Teorema de Chevalley-Warning.

Demostración 2. Sea $\{\{a_1, \ldots, a_{2p-1}\}\}$ una secuencia de elementos en el campo finito $\mathbb{Z}_p$ y consideremos el siguiente sistema de polinomios definido por:

$$P_1(x_1, \ldots, x_{2p-1}) = \sum_{i=1}^{2p-1} a_i x_i^{p-1} = 0, \tag{1.38}$$

$$P_2(x_1, \ldots, x_{2p-1}) = \sum_{i=1}^{2p-1} x_i^{p-1} = 0, \tag{1.39}$$

donde P_1, P_2 en $\mathbb{Z}_p[x_1, \ldots, x_{2p-1}]$.

Observe que:

$$grad(P_1) = grad(P_2) = p - 1$$

y

$$grad(P_1) + grad(P_2) = 2p - 2 < 2p - 1.$$

Sea N el número de soluciones de este sistema de polinomios, luego por el Teorema 1.4 tenemos que:

$$N \equiv 0\,(mod\ p). \tag{1.40}$$

Como $(0, \ldots, 0) \in \mathbb{Z}_p^{2p-1}$ es solución del sistema tenemos que $N \geq 1$.

Por lo tanto, existe una solución no trivial $(y_1, \ldots, y_{2p-1}) \in \mathbb{Z}_p^{2p-1}$ del sistema, donde al menos $y_j \neq 0$ para algún $j \in \{1, \ldots, 2p-1\}$.

Así,

$$P_1(y_1, \ldots, y_{2p-1}) = \sum_{i=1}^{2p-1} a_i y_i^{p-1} = 0, \tag{1.41}$$

$$P_2(y_1, \ldots, y_{2p-1}) = \sum_{i=1}^{2p-1} y_i^{p-1} = 0. \tag{1.42}$$

Recordemos que por el Pequeño Teorema de Fermat para cada $y \in \mathbb{Z}_p$ no nulo, $y^{p-1} \equiv 1\,(mod\ p)$; de esto se sigue que en la ecuación (1.42), $y_j \neq 0$ para exactamente p variables $y_{j_1}, \ldots, y_{j_p}$.

Luego en la ecuación (1.41) tenemos que:

$$\sum_{i=1}^{p} a_{j_i} y_{j_i}^{p-1} = 0, \tag{1.43}$$

y así:

$$\sum_{i=1}^{p} a_{j_i} = 0. \tag{1.44}$$

Por lo tanto, la subsecuencia buscada es $\{\{a_{j_1}, \ldots, a_{j_p}\}\}$. □

La siguiente demostración del Teorema de Erdös, Ginzburg y Ziv fue encontrada por Redmond y Ryavec [36] e independientemente de Blokhuis [5] y Gao [17], aquí presentamos la demostración que aparece en la referencia [1] en cuya demostración se usa el Teorema de Lucas.

Demostración 3. Sea $\{\{a_1, \ldots, a_{2p-1}\}\}$ una secuencia de $\mathbb{Z}_p$, $J = \{1, \ldots, 2p-1\}$ y consideremos la suma:

$$\begin{aligned}
S &= \sum_{I\subseteq J, |I|=p} \left(\sum_{i\in I} a_i\right)^{p-1} \\
&= \sum_{I\subseteq J, |I|=p} (a_{i_1} + \cdots + a_{i_p})^{p-1} \\
&= \sum_{I\subseteq J, |I|=p} \left(\sum_{k_1+\cdots+k_p=p-1} \frac{(p-1)!}{k_1! \ldots k_p!} a_{i_1}^{k_1} \ldots a_{i_p}^{k_p} \right) \\
&= \sum_{I\subseteq J, |I|=p} \left(\sum_{k_1+\cdots+k_p=p-1} \binom{p-1}{k_1 \ldots k_p} \prod_{j=1}^{p} a_{i_j}^{k_j} \right) \\
&= \sum_{I\subseteq J, |I|=p} \left(\sum_{k_1+\cdots+k_p=p-1} \left(\binom{k_1}{k_2} \cdots \binom{p-1}{k_p} \right) \prod_{j=1}^{p} a_{i_j}^{k_j} \right) \\
&= \sum_{I\subseteq J, |I|=p} \left(\sum_{k_1+\cdots+k_p=p-1} \prod_{i=1}^{p} \binom{\sum_{t=1}^{i} k_t}{k_i} \prod_{j=1}^{p} a_{i_j}^{k_j} \right).
\end{aligned}$$

De aquí tenemos que S se puede escribir como la suma de monomios de la forma $c\prod_{i\in J} a_i^{k_i}$, donde $\sum k_i = p-1$.

En cada tal monomio el número de números positivos k_i es algún j que satisface $1 \leq j \leq p-1$. Por lo tanto, el número de distintos subconjuntos $I \subseteq J$ de tamaño p que contribuyen al coeficiente de éste monomio en la suma S es $\binom{2p-1-j}{p-j}$, el cual es congruente con cero módulo p, como se muestra en el Teorema 1.6 tomando $h = 1$.

Dado que cada subconjunto $I \subseteq J$ contribuye lo mismo, esto implica que la suma $S \equiv 0\,(mod\ p)$.

Por otro lado, supongamos que no existe un subconjunto $I \subseteq J$ de cardinalidad p tal que $\sum_{i\in I} a_i = 0$ entonces, por el Pequeño Teorema de Fermat, cada uno de los

$\begin{pmatrix} 2p-1 \\ p \end{pmatrix}$ conjuntos I contribuye en $1(mod\ p)$ a la suma S; así que:

$$S \equiv \begin{pmatrix} 2p-1 \\ p \end{pmatrix} (mod\ p).$$

Y por el Teorema 1.6 tenemos que

$$S \equiv \begin{pmatrix} 2p-1 \\ p \end{pmatrix} (mod\ p) \equiv 1\,(mod\ p).$$

En contradicción con lo anterior.

Por lo tanto, existe $I \subseteq J$, de cardinalidad p, tal que $\sum_{i \in I} a_i = 0$.

□

Por último, presentamos la demostración del Teorema de Erdös, Ginzburg y Ziv usando el permanente de una matriz con base en la referencia [1].

Demostración 4. Sea $\{\{a_1, \ldots, a_{2p-1}\}\}$ una secuencia de elementos en el campo finito $\mathbb{Z}_p$. Renumeramos los elementos a_i de tal modo que

$$0 \leq a_1 \leq \cdots \leq a_{2p-1} < p.$$

Si $a_i = a_{i+p-1}$ para algún $i \in \{1, \ldots, p-1\}$, entonces la secuencia buscada es $a_i, a_{i+1}, \ldots, a_{i+p-1}$.

En otro caso, definamos $b_i = a_i - a_{i+p-1}$ el cual es no nulo para todo $1 \leq i \leq p-1$, y sea $\{c_1, \ldots, c_{p-1}\}$ el conjunto de todos los elementos de $\mathbb{Z}_p$, excepto el elemento formado por la suma $-a_p - a_{p+1} - \cdots - a_{2p-1}$.

Consideremos la matriz $A = (a_{ij})$ de tamaño $(p-1)\times(p-1)$, definida por $a_{ij} = b_j$, para todo $1 \leq i, j \leq p-1$.

Por la construcción de la matriz y la Proposición 1.2, es claro que:

$$per(A) = (p-1)! \cdot \prod_{j=1}^{p-1} b_j \neq 0. \tag{1.45}$$

Por lo tanto, por el Lema 1.3 existen $\epsilon_1, \ldots, \epsilon_{p-1}$ en $\{0, 1\}$ tales que la suma $\sum_{j=1}^{p-1} \epsilon_j b_j$ difiere de cada c_i y así esta suma es igual a $-a_p - a_{p+1} - \cdots - a_{2p-1}$.

De esto se sigue que en $\mathbb{Z}_p$,

$$\sum_{j=1}^{p-1} \epsilon_j b_j = -a_p - a_{p+1} - \cdots - a_{2p-1},$$

$$\sum_{j=1}^{p-1} \epsilon_j (a_j - a_{j+p-1}) = -\sum_{j=1}^{p-1} a_{j+p-1} - a_{2p-1},$$

$$a_{2p-1} + \sum_{i=1}^{p-1} [a_{i+p-1} + \epsilon_i (a_i - a_{i+p-1})] = 0,$$

y como cada término $a_{i+p-1} + \epsilon_i(a_i - a_{i+p-1})$ es o bien a_{i+p-1} o a_i, se obtiene la subsecuencia cuya suma de sus elementos es $0 \in \mathbb{Z}_p$, como queríamos.

□

CAPÍTULO 2

CONJETURA DE KEMNITZ

El Teorema de Erdös, Ginzburg y Ziv tiene varias extensiones y generalizaciones; el primero que se interesó por estudiar el problema general es H. Harborth [23] en el año de 1973; de otro lado, J. Olson [31] en el año de 1976, generaliza el resultado de Erdös, Ginzburg y Ziv, agregando ciertas condiciones adicionales a dicho teorema, por ejemplo considerar una secuencia donde ningún elemento se repite más de $n+1$ veces, entonces el conjunto de sumas y subsecuencias de tamaño n de la secuencia dada contiene un subgrupo no nulo. Estas ideas motivaron a muchos autores a estudiar problemas similares, cambiando ciertas condiciones del problema original; existe mucha literatura referente a esto, pero nosotros nos vamos a centrar en el problema bidimensional conocido como la conjetura de Kemnitz el cual surge del problema multidimensional que enuncia H. Harborth [23] de la siguiente manera:

Sea $\mathbb{Z}_n^d$ la suma directa de d copias del grupo aditivo $\mathbb{Z}_n$ de enteros módulo n, sea $s(n,d)$ el menor entero s tal que cualquier secuencia con s elementos de $\mathbb{Z}_n^d$ contiene una subsecuencia de tamaño n cuya suma de elementos es congruente con cero módulo n, el problema consiste en hallar $s(n,d)$ con la propiedad descrita.

Se tiene como resultado que $s(n,1) = 2n-1$ (Teorema de Erdös, Ginzburg y Ziv). Kemnitz en [24] conjeturó en el año de 1983 que $s(n,2) = 4n-3$ para todo n, demostró además que para los casos $n = 2,3,5,7$ la conjetura es verdadera y por lo tanto para todo n de la forma $n = 2^a 3^b 5^c 7^d$, donde a,b,c,d son enteros no negativos [24].

2.1. Valor de la función $s(p,2)$ para $p=2$ y $p=3$

En esta sección vamos a mostrar en detalle que $s(p,2) = 4p-3$, para los casos cuando $p=2$ y $p=3$ analizando el problema desde un punto de vista geométrico con base en el texto [15], en el cual se describe este problema como una aplicación del Principio del Palomar[1]; para ello, primero consideremos las siguientes definiciones.

Definición 2.1. Un **punto entero** en el plano es un punto de coordenadas enteras; es decir, un punto $P=(x,y) \in \mathbb{Z}\times\mathbb{Z}$

Definición 2.2. Dado un conjunto $\mathcal{A}=\{P_1,\ldots,P_k\}$ de k puntos enteros en el plano, donde $P_i=(x_i,y_i)\in\mathbb{Z}\times\mathbb{Z}$, para $i=1,\ldots,k$, definimos su ***centroide*** ó k***-centroide*** como el punto:

$$\frac{1}{k}\sum_{i=1}^{k} P_i := \left(\frac{1}{k}\sum_{i=1}^{k} x_i, \frac{1}{k}\sum_{i=1}^{k} y_i\right). \tag{2.1}$$

Por ejemplo, el centroide de dos puntos es su punto medio.

Definición 2.3. Decimos que un subconjunto no vacío $\mathcal{P}$ de $\mathbb{Z}\times\mathbb{Z}$ tiene k**-centroide entero** si existe $\mathcal{A}=\{P_1,\ldots,P_k\}\subseteq\mathcal{P}$ tal que el centroide de $\mathcal{A}$ es un punto entero. En caso contrario, decimos que $\mathcal{P}$ es libre de k- centroide entero.

El problema que surge entonces es: dado k fijo, ¿cuál es el mínimo cardinal de un conjunto de puntos enteros requerido para garantizar que este tiene k-centroide entero? Es decir, determinar el menor número entero positivo $s(k,2)$ tal que dados cualquier s puntos enteros en el plano existen k de ellos cuyo centroide también es un punto entero.

En consecuencia estudiaremos la función:

$$s(k,2) := \text{mín}\{|\mathcal{P}| : \mathcal{P}\subset\mathbb{Z}\times\mathbb{Z} \text{ y } \mathcal{P} \text{ tiene k-centroide entero}\}, \tag{2.2}$$

la cual existe por las cotas triviales:

$$4(k-1)+1 \leq s(k,2) \leq (k-1)k^2+1. \tag{2.3}$$

[1]También llamado Principio de Dirichlet o de las caja, que en su versión más sencilla afirma que: *si $k+1$ objetos son repartidos en k casillas entonces al menos una casilla debe contener por lo menos dos objetos.*

dadas por H. Harborth en [23] y que explicaremos con más detalle en el capítulo 3.

Analicemos la función (2.2) para algunos valores de k.

Por ejemplo, para el caso de $k = 2$, por las cotas dadas en (2.3) tenemos que $s(k, 2) = 5$, la demostración la hacemos a continuación.

Con el siguiente ejemplo mostramos que $s(2, 2) > 4$.

Ejemplo 2.1. El conjunto $\mathcal{P} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ es libre de 2-centroide entero.

En este caso, ninguno de los $\begin{pmatrix} 4 \\ 2 \end{pmatrix} = 6$ subconjuntos de $\mathcal{P}$ de cardinalidad 2 tienen 2-centroide entero o la suma de sus elementos componente a componente produce un modelo de la forma $(0 \ mod \ 2, 0 \ mod \ 2)$.

La siguiente proposición nos muestra que $s(2, 2) \leq 5$. La demostración está basada en el Principio del Palomar, la versión que usaremos de este principio es tomada del texto [15] y la enunciamos en el siguiente teorema.

Teorema 2.1. *Sean A, B dos conjuntos no vacíos tales que $|A| = n$, $|B| = k$ y una aplicación $f : A \to B$.*

(a) Entonces, sea cual sea la aplicación f, si $n > k$ existen al menos dos elementos de A, a_1, a_2 $(a_1 \neq a_2)$ tales que $f(a_1) = f(a_2)$.

(b) O, en términos más generales, si $n > kr$, para cierto $r \geq 1$, hay al menos $r + 1$ elementos distintos de A, $a_1, a_2, \ldots, a_r$, tales que

$$f(a_1) = f(a_2) = \cdots = f(a_r).$$

Así, enunciamos la siguiente proposición:

Proposición 2.1. *Todo conjunto de puntos enteros en el plano con 5 o más elementos tiene 2-centroide entero.*

Demostración. Sea $\mathcal{P} = \{P_1, \ldots, P_5\} \subseteq \mathbb{Z} \times \mathbb{Z}$, donde $P_i = (x_i, y_i),\ i = 1, \ldots, 5$. Vamos a probar que existen i, j distintos, $1 \leq i, j \leq 5$, tales que el punto medio del segmento $\overline{P_i P_j}$ es un punto entero.

Definamos la función $f : \mathcal{P} = \{P_1, \ldots, P_5\} \to \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ tal que $f(P_i) = (x_i \ mod \ 2, y_i \ mod \ 2)$, para cada $i = 1, \ldots, 5$.

Como $|\mathcal{P}| = 5$, por el Principio del Palomar existen al menos $\lceil \frac{5}{4} \rceil = 2$ puntos que tienen la misma imagen[2]; es decir, existen $i \neq j$ tales que $f(P_i) = f(P_j)$. Claramente el segmento $\overline{P_iP_j}$ tiene punto medio entero ya que x_i y x_j tienen la misma paridad, al igual que y_i y y_j. □

Por lo tanto, del Ejemplo 2.1 y la Proposición 2.1 concluimos que $s(2,2) = 5$.

Ahora estudiemos el caso para $k = 3$, el problema consiste entonces en determinar el menor entero $s(3,2)$ que obliga a la existencia de un 3-centroide entero; en la explicación que damos a continuación nos podemos dar cuenta que el problema para $k = 3$ se vuelve más complicado pues el Principio del Palomar no es suficiente para la demostración.

Primero, consideremos el siguiente ejemplo:

Ejemplo 2.2. El conjunto $\mathcal{P} = \{(0,0), (0,3), (0,1), (0,4), (1,0), (4,0), (1,1), (1,4)\}$ es libre de 3-centroide entero.

En este ejemplo tenemos que ninguno de los $\begin{pmatrix} 8 \\ 3 \end{pmatrix} = 56$ subconjuntos de 3 elementos de $\mathcal{P}$ tiene 3-centroide entero, pues los modelos módulo 3 componente a componente de los ocho puntos son $\{(0,0), (0,1), (1,0), (1,1)\}$, cada elemento con multiplicidad 2 y a partir de ellos no es posible tener que la suma de tres puntos de $\mathcal{P}$ produzca un modelo de la forma $(0 \ mod \ 3, 0 \ mod \ 3)$.

Así, $s(3,2) > 8$.

La siguiente proposición nos muestra que $s(3,2) \leq 13$ cuya demostración está solamente basada en el Principio del Palomar.

Proposición 2.2. *Todo conjunto de puntos enteros en el plano con 13 o más elementos tiene 3-centroide entero.*

Demostración. Sea $\mathcal{P} = \{P_1, \ldots, P_{13}\} \subseteq \mathbb{Z} \times \mathbb{Z}$, donde $P_i = (x_i, y_i)$, para cada $i = 1, \ldots, 13$. Vamos a probar que existen i, j, k distintos, $1 \leq i, j, k \leq 13$, tales que el centroide de los puntos P_i, P_j, P_k es un punto entero.

Consideremos la función $f : \mathcal{P} = \{P_1, \ldots, P_{13}\} \to \{0, 1, 2\}$ tal que

$f(P_i) = x_i \ mod \ 3$, para cada $i = 1, \ldots, 13$.

Como $|\mathcal{P}| = 13$, por el Principio del Palomar existen al menos $\lceil \frac{13}{3} \rceil = 5$ puntos de $\mathcal{P}$ que tiene la misma imagen, digamos que son $P_1, \ldots, P_5$.

[2]Aquí $\lceil x \rceil$ que denota el menor entero mayor o igual que x.

Ahora analicemos las segundas componentes en módulo 3 de éstos cinco puntos. Si tres de estas segundas componentes están en distintas clases residuales, los tres puntos correspondientes tiene 3-centroide entero. Si este no es el caso; es decir, si alguna de las tres clases módulo 3 tiene preimagen vacía, de nuevo por el Principio del Palomar, existen por lo menos $\lceil \frac{5}{2} \rceil = 3$ puntos cuyas segundas componentes están en la misma clase módulo 3. Luego, los tres puntos correspondientes tienen 3-centroide entero. □

Hasta aquí del Ejemplo 2.2 y la Proposición 2.2 tenemos que $9 \leq s(3,2) \leq 13$.

Sin embargo, tenemos que $s(3,2) = 9$ y como lo mencionamos anteriormente, el Principio del Palomar no es suficiente para probar esta afirmación, se necesitan otros argumentos por ejemplo el uso del Plano Proyectivo como lo describen en el texto [15]. Aquí presentamos una reconstrucción de esta prueba.

De esta manera, tenemos el siguiente teorema:

Teorema 2.2. *Todo conjunto de puntos enteros en el plano con 9 o más elementos tiene 3-centroide entero.*

Demostración. Sea $\mathcal{P} = \{P_1, \ldots, P_9\} \subseteq \mathbb{Z} \times \mathbb{Z}$, vamos a probar que existen tres puntos de $\mathcal{P}$, $P_i = (x_i, y_i)$, $P_j = (x_j, y_j)$, $P_k = (x_k, y_k)$ con i, j, k en $\{1, \ldots, 9\}$ tales que

$$x_i \equiv x_j \equiv x_k (mod\ 3) \text{ o } \{x_i (mod\ 3), x_j (mod\ 3), x_k (mod\ 3)\} = \{0, 1, 2\}, \text{ y}$$

$$y_i \equiv y_j \equiv y_k (mod\ 3) \text{ o } \{y_i (mod\ 3), y_j (mod\ 3), y_k (mod\ 3)\} = \{0, 1, 2\}.$$

Los nueve posibles puntos enteros módulo 3 distintos, que podemos obtener son todos los elementos de $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, los cuales están representados en la siguiente gráfica.

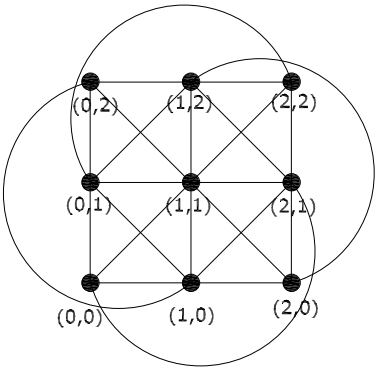

Figura 1. Puntos de $\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Las doce líneas de la Figura 1. corresponden a tripletas de puntos que determinan un 3-centroide entero. Modulando los nueve puntos de $\mathcal{P}$, en módulo 3, pueden suceder los siguientes casos:

- Si tres de los puntos de $\mathcal{P}$ están en la misma clase residual, entonces los tres puntos correspondientes tienen 3-centroide entero.
- Si este no es el caso, supongamos que a lo más dos puntos enteros de $\mathcal{P}$ caen en la misma clase residual, por el Principio del Palomar, tenemos al menos $\lceil \frac{9}{2} \rceil = 5$ puntos en clases residuales distintas.

  Observemos a continuación que de estos cinco puntos, tres tienen centroide entero, para ello trabajemos con las clases residuales.

  Por ejemplo, supongamos que tres de estos cinco puntos son $(0,0), (0,1), (1,1)$, que no tienen 3-centroide entero.

  - Si los dos puntos que faltan están en el conjunto $\{(0,2), (2,1), (2,2)\}$ entonces se obtienen puntos colineales y los puntos correspondientes a ellos tienen 3-centroide entero.
  - Si este no es el caso, los dos puntos que faltan pueden ser escogidos de: $\{(1,0), (1,2), (2,0)\}$, pero si escogemos $\{(1,0), (1,2)\}$ ó $\{(1,0), (2,0)\}$ tenemos de nuevo puntos colineales y los puntos correspondientes a ellos tienen 3-centroide entero. O si escogemos $\{(1,2), (2,0)\}$, con el punto $(0,1)$ los puntos correspondientes a ellos tienen 3-centroide entero.

Las demás opciones se prueban análogamente. □

2.2. Valor de la función $s(k,2)$ para $k=4$ y $k=6$

Como mencionamos anteriormente esta conjetura es multiplicativa, así que usando el hecho que $s(2,2)=5$ y $s(3,2)=9$ vamos a demostrar que $s(4,2)=13$ y $s(6,2)=21$.

Ejemplo 2.3. El conjunto formado por tres copias de cada uno de los puntos $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ en módulo 4 es libre de 4-centroide entero, pues a partir de ellos no es posible tener que la suma de cuatro puntos produzca un modelo de la forma $(0\ mod\ 4, 0\ mod\ 4)$.

Así, $s(4,2)>12$.

Teorema 2.3. *Todo conjunto de puntos enteros en el plano con 13 o más elementos tiene 4-centroide entero.*

Demostración. Vamos a probar que $s(4,2)\leq 13$.

Sea $\mathcal{P}=\{P_1,\ldots,P_{13}\}$, escogemos cinco puntos de $\mathcal{P}$, de ellos existen dos puntos, digamos P_1,P_2, cuyo 2-centroide

$$S_1=\frac{P_1+P_2}{2}$$

es un punto entero.

Sea $\mathcal{P}_1=\mathcal{P}\setminus\{P_1,P_2\}$, así $|\mathcal{P}_1|=11$. Entre estos once puntos escogemos cinco, de ellos existen dos puntos, digamos P_3,P_4, cuyo 2-centroide

$$S_2=\frac{P_3+P_4}{2}$$

es un punto entero.

Sea $\mathcal{P}_2=\mathcal{P}_1\setminus\{P_3,P_4\}$, así $|\mathcal{P}_2|=9$. Entre estos nueve puntos escogemos cinco, de ellos existen dos puntos, digamos P_5,P_6, cuyo 2-centroide

$$S_3=\frac{P_5+P_6}{2}$$

es un punto entero.

Sea $\mathcal{P}_3=\mathcal{P}_2\setminus\{P_5,P_6\}$, así $|\mathcal{P}_3|=7$. Entre estos siete puntos escogemos cinco, de ellos existen dos puntos, digamos P_7,P_8, cuyo 2-centroide

$$S_4=\frac{P_7+P_8}{2}$$

es un punto entero.

Sea $\mathcal{P}_4 = \mathcal{P}_3 \setminus \{P_7, P_8\}$, así $|\mathcal{P}_4| = 5$. Entre estos cinco puntos existen dos de ellos, digamos P_9, P_{10}, cuyo 2-centroide

$$S_5 = \frac{P_9 + P_{10}}{2}$$

es un punto entero.

Ahora bien, entre los cinco puntos $S_1, \ldots, S_5$, existen dos, digamos S_1, S_2, cuyo 2-centroide

$$\frac{S_1 + S_2}{2} = \frac{\frac{P_1+P_2}{2} + \frac{P_3+P_4}{2}}{2} = \frac{P_1 + P_2 + P_3 + P_4}{4}$$

es un punto entero.

Luego, de $\mathcal{P}$ existen cuatro puntos P_1, P_2, P_3, P_4, cuyo 4-centroide es un punto entero. □

Ahora estudiemos el caso para $p = 6$.

Ejemplo 2.4. El conjunto formado por cinco copias de cada uno de los puntos $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ en módulo 6 es libre de 6-centroide entero, pues a partir de ellos no es posible tener que la suma de seis puntos produzca un modelo de la forma $(0 \ mod \ 6, 0 \ mod \ 6)$.

Así, $s(6, 2) > 20$.

Teorema 2.4. *Todo conjunto de puntos enteros en el plano con 21 o más elementos tiene 6-centroide entero.*

Demostración. Vamos a probar que $s(6, 2) \leq 21$.

Sea $\mathcal{P} = \{P_1, \ldots, P_{21}\}$, escogemos nueve puntos de $\mathcal{P}$, de ellos existen tres puntos, digamos P_1, P_2, P_3, cuyo 3-centroide

$$S_1 = \frac{P_1 + P_2 + P_3}{3}$$

es un punto entero.

Sea $\mathcal{P}_1 = \mathcal{P} \setminus \{P_1, P_2, P_3\}$, así $|\mathcal{P}_1| = 18$. Entre estos dieciocho puntos escogemos nueve, de ellos existen tres puntos, digamos P_4, P_5, P_6, cuyo 3-centroide

$$S_2 = \frac{P_4 + P_5 + P_6}{3}$$

es un punto entero.

Sea $\mathcal{P}_2 = \mathcal{P}_1 \setminus \{P_4, P_5, P_6\}$, así $|\mathcal{P}_2| = 15$. Entre estos quince puntos escogemos nueve, de ellos existen tres puntos, digamos P_7, P_8, P_9, cuyo 3-centroide

$$S_3 = \frac{P_7 + P_8 + P_9}{3}$$

es un punto entero.

Sea $\mathcal{P}_3 = \mathcal{P}_2 \setminus \{P_7, P_8, P_9\}$, así $|\mathcal{P}_3| = 12$. Entre estos doce puntos escogemos nueve, de ellos existen tres puntos, digamos P_{10}, P_{11}, P_{12}, cuyo 3-centroide

$$S_4 = \frac{P_{10} + P_{11} + P_{12}}{3}$$

es un punto entero.

Sea $\mathcal{P}_4 = \mathcal{P}_3 \setminus \{P_{10}, P_{11}, P_{12}\}$, así $|\mathcal{P}_4| = 9$. Entre estos nueve puntos existen tres de ellos, digamos P_{13}, P_{14}, P_{15}, cuyo 3-centroide

$$S_5 = \frac{P_{13} + P_{14} + P_{15}}{3}$$

es un punto entero.

Ahora bien, entre los cinco puntos $S_1, \ldots, S_5$, existen dos, digamos S_1, S_2, cuyo 2-centroide

$$\frac{S_1 + S_2}{2} = \frac{\frac{P_1+P_2+P_3}{3} + \frac{P_4+P_5+P_6}{3}}{2} = \frac{P_1 + P_2 + P_3 + P_4 + P_5 + P_6}{6}$$

es un punto entero.

Luego, de $\mathcal{P}$ existen seis puntos $P_1, P_2, P_3, P_4, P_5, P_6$, cuyo 6-centroide es un punto entero. □

De lo anterior podemos notar que la conjetura es multiplicativa, lo cual fue demostrado también por Kemnitz en [24].

Es decir, Kemnitz demostró que si la función $s(k, 2)$ es verdadera para un par de enteros, también es verdadera para su producto, por tal razón es suficiente verificarla para el caso cuando n es primo, como lo mostramos en el siguiente teorema.

Teorema 2.5. *Si* $n = pq$, $s(p, 2) = 4p - 3$ *y* $s(q, 2) = 4q - 3$ *entonces*

$$s(n, 2) = 4n - 3. \tag{2.4}$$

Demostración. Sea $\mathcal{P} = \{R_1, \ldots, R_{4n-3}\} \subseteq \mathbb{Z} \times \mathbb{Z}$, como $|\mathcal{P}| = 4n-3 = 4pq-3$ y supongamos que $p < q$; escogemos $4q-3$ elementos de $\mathcal{P}$, de ellos existen q puntos, digamos $R_1, \ldots, R_q$, cuyo centroide

$$S_1 = \frac{R_1 + \cdots + R_q}{q}$$

es un punto entero.

Sea $\mathcal{P}_1 = \mathcal{P} \setminus \{R_1, \ldots, R_q\}$, así $|\mathcal{P}_1| = 4pq-3-q = (4p-1)q-3$. De los elementos de $\mathcal{P}_1$ escogemos $4q-3$, de ellos existen q puntos, digamos $R_{q+1}, \ldots, R_{2q}$, cuyo centroide

$$S_2 = \frac{R_{q+1} + \cdots + R_{2q}}{q}$$

es un punto entero.

Sea $\mathcal{P}_2 = \mathcal{P}_1 \setminus \{R_{q+1}, \ldots, R_{2q}\}$, así $|\mathcal{P}_2| = (4p-1)q-3-q = (4p-2)q-3$ y continuando con el proceso después de $(4p-4)$ pasos nos quedan

$$[4p-(4p-4)]q-3 = 4q-3$$

elementos; de ellos existen q cuyo centroide

$$S_{4p-3} = \frac{R_{(4p-4)q+1} + \cdots + R_{(4p-3)q}}{q}$$

es un punto entero.

Ahora, tenemos $4p-3$ puntos enteros, $S_1, \ldots, S_{4p-3}$, de ellos existen p, digamos $S_1, \ldots, S_p$, cuyo centroide

$$\frac{S_1 + \cdots + S_p}{p} = \frac{\frac{R_1+\cdots+R_q}{q} + \cdots + \frac{R_{(p-1)q+1}+\cdots+R_{pq}}{q}}{p} = \frac{R_1 + \cdots + R_{pq}}{pq}$$

es un punto entero.

Luego, existen $pq = n$ elementos de $\mathcal{P}$ cuyo k-centroide es un punto entero, los cuales son $R_1, \ldots, R_{pq}$. □

2.3. Valor de la función $s(p,2)$ para $p = 5$ y $p = 7$

Ahora vamos a calcular los valores de $s(5,2)$ y $s(7,2)$ con base en el artículo de Kemnitz [24]; en este artículo se muestra el caso cuando $p = 5$ y en nuestro trabajo realizamos los cálculos para $p = 7$ que no están reportados en la literatura.

Para la prueba de $s(5,2)$ y $s(7,2)$ Kemnitz introduce la función $g(p,2)$, la cual es válida para todo entero mayor que 2 y se define de la siguiente manera: sea $g(p,2)$ el mínimo cardinal de un conjunto contenido en $\mathbb{Z}_p \oplus \mathbb{Z}_p$, tal que este conjunto contiene un subconjunto de tamaño p cuya suma de elementos es congruente con $(0,0)$ módulo p. Al conjunto con estas características lo llamaremos conjunto con suma cero; en caso contrario, diremos que el conjunto es libre de suma cero.

En este caso, estudiaremos la función $g(p,2)$ para los valores de $p = 5$ y $p = 7$; sin embargo, la existencia de esta función para todo p impar se garantiza por las siguientes cotas:

$$2p - 1 \leq g(p,2) \leq (p-1)p + 1. \tag{2.5}$$

Verifiquemos las anteriores cotas.

Para la cota inferior de (2.5), veamos algunos ejemplos de conjuntos libres de suma cero.

- Para $p = 3$ el conjunto $\mathcal{P} = \{(0,0),(1,0),(0,1),(1,1)\}$, es libre de suma cero; así, $g(3,2) \geq 5$.
- Para $p = 5$ el conjunto

  $\mathcal{P} = \{(0,0),(1,0),(2,0),(3,0),(0,1),(1,1),(2,1),(3,1)\}$,

  es libre de suma cero; así, $g(5,2) \geq 9$.
- Para $p = 7$ el conjunto

  $\mathcal{P} = \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(0,1),(1,1),(2,1),(3,1),$
  $(4,1),(5,1)\}$, es libre de suma cero; así, $g(7,2) \geq 13$.

En general, para cualquier $p \geq 3$ impar basta tomar un conjunto con $(p-1)$ puntos cuyas primeras coordenadas (o segundas) sean todas 0 y cuyas segundas coordenadas (o primeras) sean todas diferentes, más $(p-1)$ puntos cuyas primeras coordenadas (o segundas) sean todas 1 y cuyas segundas coordenadas (o primeras) sean todas diferentes. El conjunto con estas características es libre de suma cero, por lo tanto tenemos que $g(p,2) \geq 2p-1$ para todo $p \geq 3$ impar.

Para la cota superior de (2.5), tomemos un subconjunto $\mathcal{P} = \{Q_1, \ldots, Q_{(p-1)p+1}\}$ de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ y consideremos la función $f : \mathcal{P} \to \{0,1,\ldots,p-1\}$ definida por:

$f(Q_i) = x_i (mod\ p)$, para cada $i = 1, \ldots, (p-1)p+1$.

Por el Principio del Palomar al menos $\left\lceil \frac{(p-1)p+1}{p} \right\rceil = \left\lceil (p-1) + \frac{1}{p} \right\rceil = p$ puntos tienen la primera coordenada en la misma clase residual módulo p, digamos que estos puntos son $Q_1, \ldots, Q_p$.

Ahora analicemos la segunda coordenada de estos p puntos, para ello consideremos la función $\tilde{f} : \{Q_1, \ldots, Q_p\} \to \{0, 1, \ldots, p-1\}$ tal que $\tilde{f}(Q_i) = y_i (mod\ p)$.

Si cada punto tiene distinta imagen, los puntos correspondientes tienen suma cero pues p es impar. Si este no es el caso; es decir, si existe un elemento en el codominio que tiene preimagen vacía, de nuevo por el Principio del Palomar, existen al menos $\left\lceil \frac{p}{p-1} \right\rceil = 2$ puntos que tienen la misma imagen, pero esto no puede ser posible pues todos los puntos de $\mathcal{P}$ son distintos.

Por lo tanto, el subconjunto que tiene suma cero es $\{Q_1, \ldots, Q_p\}$.

Para calcular $g(5, 2)$ y $g(7, 2)$ vamos a tener en cuenta la siguiente terminología usada por Kemnitz [24].

Si p puntos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ tienen suma cero, llamaremos a esto una ***p-linea*** y dados s puntos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$, un ***s-esquema*** consiste de un arreglo de dos filas y s columnas. Esto es, dados $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, ..., $P_s = (x_s, y_s)$ en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ el s-esquema es el siguiente arreglo

$$\begin{array}{cccc} x_1 & x_2 & \cdots & x_s \\ y_1 & y_2 & \cdots & y_s \end{array}$$

Decimos que dos s-esquemas A y B son *equivalentes* si satisfacen alguna de las siguientes condiciones:

- Si B se obtiene al intercambiar dos columnas o dos filas de A.
- Si B se obtiene al multiplicar una fila de A con 1, 2, ... , $p-1$.
- Si B se obtiene al agregar a una fila de A el vector $(v, v, \ldots, v)$, de tamaño s.
- Si B se obtiene al sumar una fila con otra de A.

Igualmente, dos s-esquemas son equivalentes si y sólo si la existencia de una p-linea en uno de ellos implica una p-linea en el otro y viceversa.

Además, para la prueba de $g(5, 2)$ y $g(7, 2)$ usaremos la función $A_p(s, t)$ que representa el mínimo número de sumas incongruentes módulo p, que se obtiene al sumar de cualquier manera s enteros tomados de un conjunto de t enteros incongruentes por pares módulo p, para $1 \leq s \leq t \leq p$. Para el caso $p = 7$ realicé todos los cálculos y demostré que la conjetura es verdad, este resultado es propio de mi trabajo puesto en la literatura no aparece.

Vale la pena aclarar que no existe ninguna fórmula general para determinar el valor de $A_p(s, t)$ para un primo p arbitrario dado. En nuestro caso, como ya mencionamos, sólo vamos a trabajar con $p = 5$ y $p = 7$.

En las dos tablas siguientes mostramos los valores de $A_5(s,t)$ y $A_7(s,t)$; la Tabla 1., que corresponde al caso $p = 5$, fue tomada de [24], de la cual realicé los cálculos pertinentes para comprobarla; para la Tabla 2., que es el caso $p = 7$, si realicé todos los cálculos correspondientes, los cuales son usados más adelante para la demostración de $s(7,2)$.

$s \diagdown t$	1	2	3	4	5
1	1	2	3	4	5
2		1	3	5	5
3			1	4	5
4				1	5
5					1

TABLA 1. Función $A_5(s,t)$

$s \diagdown t$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2		1	3	5	7	7	7
3			1	4	7	7	7
4				1	5	7	7
5					1	6	7
6						1	7
7							1

TABLA 2. Función $A_7(s,t)$

Para la prueba de la siguiente proposición nos basamos en [24].

Proposición 2.3. *Para $p = 5$ tenemos que:*

$$g(5,2) = 9. \tag{2.6}$$

Demostración. Sea $\mathcal{P} = \{a_1, \ldots, a_9\} \subseteq \mathbb{Z}_5 \oplus \mathbb{Z}_5$

Por la desigualdad (2.5) para $p = 5$ tenemos que $g(5,2) \geq 9$, por tal razón sólo nos hace falta verificar que 9 es una cota superior; es decir, vamos a verificar que todo 9–esquema contiene una linea.

Vamos a ubicar los nueve puntos de $\mathcal{P}$ en un 9-esquema. Si en la primera (o segunda) fila del 9-esquema aparece por lo menos cinco veces un elemento de $\mathbb{Z}_5$ entonces, como los puntos de $\mathcal{P}$ son distintos, las segundas (o primeras) coordenadas de estos puntos son todas diferentes por lo tanto la suma de las correspondientes

segundas (o primeras) coordenadas también es congruente con 0 módulo 5. Si este no es el caso, vamos a analizar los 9-esquemas que podemos obtener; por las propiedades de equivalencia de los esquemas nos podemos restringir a 9-esquemas cuya primera fila es alguna de las siguientes.

Para $2 \leq a, b, c \leq 4$ tenemos:

(a)	0	0	0	0	1	1	1	1	a
(b)	0	0	0	0	1	1	1	a	a
(c)	0	0	0	0	1	1	1	a	b
(d)	0	0	0	0	1	1	a	a	b
(e)	0	0	0	0	1	1	2	3	4
(f)	0	0	0	1	1	1	a	a	a
(g)	0	0	0	1	1	1	a	a	b
(h)	0	0	0	1	1	1	2	3	4
(i)	0	0	0	1	1	a	a	b	b
(j)	0	0	0	1	1	a	a	b	c
(k)	0	0	1	1	a	a	b	b	c

Ahora, usemos la Tabla 1. y el Teorema de Cauchy-Davenport para probar que existe una 5-linea en cada uno de estos casos.

Por ejemplo, un esquema puede contener:

- cuatro puntos cuya primera coordenada es 0,
- al menos dos puntos con 1 en la primera coordenada y
- al menos uno con 4 en la primera coordenada.

En este caso, si escogemos de ellos tres puntos con 0, uno con 1 y uno con 4 entonces la suma de las primeras coordenadas de estos cinco puntos es congruente con 0 módulo 5.

De los cuatro puntos que tiene primera coordenada 0, de acuerdo a la Tabla 1, si sumamos de cualquier manera posible tres de las segundas coordenadas de éstos cuatro puntos, obtenemos cuatro clases residuales incongruentes módulo 5; llamemos A el conjunto formado por estas cuatro clases residuales. Como además existen dos posibilidades de escoger 1 en la primera coordenada; llamemos B al conjunto formado por las dos clases residuales de las segundas coordenadas correspondientes a dichos puntos.

Ahora formamos el conjunto suma de A y B; por el Teorema de Cauchy- Davenport tenemos que:

$$|A + B| \geq min\{5, 4 + 2 - 1\} = 5$$

Es decir, $A + B = \mathbb{Z}_5$.

Además, al agregar la clase residual de la segunda coordenada del punto cuya primera coordenada es 4 obtenemos que el residuo 0 también lo podemos representar como suma de las segundas coordenadas; así conseguimos una 5-linea en el 9-esquema y en consecuencia obtenemos la subsecuencia de suma cero.

Los demás casos son tratados análogamente, por tal razón omitimos los detalles.

□

Usando el Proposición 2.3 y el siguiente Lema, debido a J. Olson [31], vamos a mostrar que $s(5, 2) = 17$.

Lema 2.1. *Sea p un primo fijo. Toda secuencia de al menos $3p-2$ puntos enteros contiene una subsecuencia de tamaño t, para algún $1 \leq t \leq p$, cuya suma de elementos es congruente con $(0, 0)$ módulo p.*

Ejemplo 2.5. El conjunto formado por cuatro copias de los puntos $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ en módulo 5 es libre de 5-centroide entero, pues a partir de ellos no es posible tener que la suma de cinco puntos produzca un modelo de la forma $(0\ mod\ 5, 0\ mod\ 5)$.

Así, $s(5, 2) > 16$.

Con base en el artículo [24] realizamos la prueba del siguiente teorema.

Teorema 2.6. *Todo conjunto de puntos enteros en el plano con 17 o más elementos tiene 5-centroide entero.*

Demostración. Por el ejemplo anterior es suficiente probar que $s(5, 2) \leq 17$.

Sea $\{a_1, \ldots, a_{17}\}$ un conjunto de puntos enteros en el plano; si entre los diecisiete puntos encontramos:

Caso 1: Por lo menos cinco puntos que pertenecen a la misma clase residual entonces los puntos correspondientes tiene 5-centroide entero.
Caso 2: Más de ocho puntos tales que por pares sean incongruentes módulo 5 en al menos una coordenada, entonces por la Proposición 2.3 existen cinco de ellos cuyo 5-centroide es entero.

Si ninguno de los casos anteriores sucede, nos podemos reducir a trabajar con puntos en $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ y sólo debemos probar la existencia de una 5-linea en el 17-esquema con las siguientes características.

Un vector aparece a lo más cuatro veces, por el caso 1; o un vector aparece a lo más $\lceil \frac{17}{8} \rceil = 3$ veces, por el caso 2. Sin perdida de generalidad, por las propiedades de equivalencia de los esquemas, supongamos que ese vector es $(0,0)\,(mod\ 5)$. Entonces tenemos al menos trece puntos diferentes del punto $(0,0)\,(mod\ 5)$; por el Lema 2.1 existen t de ellos, $1 \leq t \leq 5$, cuya suma es congruente con $(0,0)$ módulo 5. Claramente $t > 1$ y si $t = 5$ obtenemos la subsecuencia buscada. Si $2 \leq t \leq 4$, completamos la 5-linea en el 17-esquema con los vectores $(0,0)\,(mod\ 5)$ que ya teníamos. Esto completa la demostración.

□

De manera similar se verifica que $s(7,2) = 25$, en este caso hacemos un aporte para el trabajo puesto que realicé todos los cálculos correspondientes como se muestra a continuación.

Proposición 2.4. *Para $p = 7$ tenemos que:*

$$g(7,2) = 13. \tag{2.7}$$

Demostración. Sea $\mathcal{P} = \{a_1, \ldots, a_{13}\} \subseteq \mathbb{Z}_7 \oplus \mathbb{Z}_7$

Por la desigualdad (2.5) para $p = 7$ tenemos que $g(7,2) \geq 13$, por tal razón sólo nos hace falta verificar que 13 es una cota superior; es decir, vamos a verificar que todo 13-esquema contiene una 7-linea.

Vamos a ubicar los trece puntos de $\mathcal{P}$ en un 13-esquema. Si en la primera (o segunda) fila del 13-esquema aparece por lo menos siete veces un elemento de $\mathbb{Z}_7$ entonces, como los puntos de $\mathcal{P}$ son distintos, las segundas (o primeras) coordenadas de estos puntos son todas diferentes por lo tanto la suma de las correspondientes segundas (o primeras) coordenadas también es congruente con 0 módulo 7. Si este no es el caso, analicemos los 13-esquemas que podemos obtener; por las propiedades de equivalencia de los esquemas nos podemos restringir a 13-esquemas cuya primera fila es alguna de las siguientes.

Para $2 \leq a, b, c, d, e \leq 6$ tenemos:

(*1*)	0	0	0	0	0	0	1	1	1	1	1	1	a
(*2*)	0	0	0	0	0	0	1	1	1	1	1	a	a
(*3*)	0	0	0	0	0	0	1	1	1	1	1	a	b

(*4*)	0	0	0	0	0	0	1	1	1	1	a	a	a
(*5*)	0	0	0	0	0	0	1	1	1	1	a	a	b
(*6*)	0	0	0	0	0	0	1	1	1	1	a	b	c
(*7*)	0	0	0	0	0	0	1	1	1	a	a	a	b
(*8*)	0	0	0	0	0	0	1	1	1	a	a	b	b
(*9*)	0	0	0	0	0	0	1	1	1	a	a	b	c
(*10*)	0	0	0	0	0	0	1	1	1	a	b	c	d
(*11*)	0	0	0	0	0	0	1	1	a	a	b	b	c
(*12*)	0	0	0	0	0	0	1	1	a	a	b	c	d
(*13*)	0	0	0	0	0	0	1	1	2	3	4	5	6
(*14*)	0	0	0	0	0	1	1	1	1	1	a	a	a
(*15*)	0	0	0	0	0	1	1	1	1	1	a	a	b
(*16*)	0	0	0	0	0	1	1	1	1	1	a	b	c
(*17*)	0	0	0	0	0	1	1	1	1	a	a	a	a
(*18*)	0	0	0	0	0	1	1	1	1	a	a	a	b
(*19*)	0	0	0	0	0	1	1	1	1	a	a	b	b
(*20*)	0	0	0	0	0	1	1	1	1	a	a	b	c
(*21*)	0	0	0	0	0	1	1	1	1	a	b	c	d
(*22*)	0	0	0	0	0	1	1	1	a	a	a	b	b
(*23*)	0	0	0	0	0	1	1	1	a	a	a	b	c
(*24*)	0	0	0	0	0	1	1	1	a	a	b	b	c
(*25*)	0	0	0	0	0	1	1	1	a	a	b	c	d
(*26*)	0	0	0	0	0	1	1	1	2	3	4	5	6
(*27*)	0	0	0	0	0	1	1	a	a	b	b	c	c
(*28*)	0	0	0	0	0	1	1	a	a	b	b	c	d
(*29*)	0	0	0	0	0	1	1	a	a	b	c	d	e
(*30*)	0	0	0	0	1	1	1	1	a	a	a	a	b
(*31*)	0	0	0	0	1	1	1	1	a	a	a	b	b
(*32*)	0	0	0	0	1	1	1	1	a	a	a	b	c
(*33*)	0	0	0	0	1	1	1	1	a	a	b	b	c
(*34*)	0	0	0	0	1	1	1	1	a	a	b	c	d
(*35*)	0	0	0	0	1	1	1	1	2	3	4	5	6
(*36*)	0	0	0	0	1	1	1	a	a	a	b	b	b
(*37*)	0	0	0	0	1	1	1	a	a	a	b	b	c

(*38*)	0	0	0	0	1	1	1	a	a	a	b	c	d
(*39*)	0	0	0	0	1	1	1	a	a	b	b	c	c
(*40*)	0	0	0	0	1	1	1	a	a	b	b	c	d
(*41*)	0	0	0	0	1	1	1	a	a	b	c	d	e
(*42*)	0	0	0	0	1	1	a	a	b	b	c	c	d
(*43*)	0	0	0	0	1	1	a	a	b	b	c	d	e
(*44*)	0	0	0	1	1	1	a	a	a	b	b	b	c
(*45*)	0	0	0	1	1	1	a	a	a	b	b	c	c
(*46*)	0	0	0	1	1	1	a	a	a	b	b	c	d
(*47*)	0	0	0	1	1	1	a	a	a	b	c	d	e
(*48*)	0	0	0	1	1	1	a	a	b	b	c	c	d
(*49*)	0	0	0	1	1	1	a	a	b	b	c	d	e
(*50*)	0	0	0	1	1	a	a	b	b	c	c	d	d
(*51*)	0	0	0	1	1	a	a	b	b	c	c	d	e
(*52*)	0	0	1	1	a	a	b	b	c	c	d	d	e

Ahora, usemos la Tabla 2. y el Teorema de Cauchy-Davenport para probar que existe una 7-linea en cada uno de estos casos.

Por ejemplo, un esquema puede contener:

- cinco puntos cuya primera coordenada es 0,
- al menos cuatro puntos con 1 en la primera coordenada y
- al menos uno con 5 en la primera coordenada.

En este caso, si escogemos de ellos cuatro puntos con 0, dos con 1 y uno con 5 entonces la suma de las primeras coordenadas de estos siete puntos es congruente con 0 módulo 7.

De los cinco puntos que tiene primera coordenada 0, de acuerdo a la Tabla 2, si sumamos de cualquier manera posible cuatro de las segundas coordenadas de éstos cinco puntos, obtenemos cinco clases residuales incongruentes módulo 7; llamemos A el conjunto formado por estas cinco clases residuales. De los cuatro puntos que tiene 1 en la primera coordenada, de acuerdo a la Tabla 2, si sumamos de cualquier manera posible dos de las segundas coordenadas de éstos cuatro puntos, obtenemos cinco clases residuales incongruentes módulo 7; llamemos B al conjunto formado por estas cinco clases residuales de las segundas coordenadas correspondientes a dichos puntos.

Ahora formamos el conjunto suma de A y B; por el Teorema de Cauchy- Davenport tenemos que:

$$|A + B| \geq min\{7, 5 + 5 - 1\} = 7$$

Es decir, $A + B = \mathbb{Z}_7$.

Además, al agregar la clase residual de la segunda coordenada del punto cuya primera coordenada es 5 obtenemos que el residuo 0 también lo podemos representar como suma de las segundas coordenadas, así conseguimos una 7-linea en el 13-esquema y en consecuencia obtenemos la subsecuencia de suma cero.

Los demás casos son tratados análogamente.

□

Ahora estudiemos el caso de $p = 7$.

Ejemplo 2.6. El conjunto formado por seis copias de los puntos $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ en módulo 7 es libre de 7-centroide entero, pues a partir de ellos no es posible tener que la suma de siete puntos produzca un modelo de la forma $(0 \ mod \ 7, \ 0 \ mod \ 7)$.

Así, $s(7, 2) > 24$.

Teorema 2.7. *Todo conjunto de puntos enteros en el plano con 25 o más elementos tiene 7-centroide entero.*

Demostración. Por el ejemplo anterior es suficiente probar que $s(7, 2) \leq 25$.

Sea $\{a_1, \ldots, a_{25}\}$ un conjunto de puntos enteros en el plano; si entre los veinticinco puntos encontramos:

Caso 1: Por lo menos siete puntos que pertenecen a la misma clase residual entonces los puntos correspondientes tiene 7-centroide entero.
Caso 2: Más de doce puntos tales que dos a dos sean incongruentes módulo 7 en al menos una coordenada entonces por la Proposición 2.4 existen siete de ellos cuyo 7-centroide es entero.

Si ninguno de los casos anteriores sucede, nos podemos reducir a trabajar con puntos en $\mathbb{Z}_7 \oplus \mathbb{Z}_7$, sólo debemos probar la existencia de una 7-linea en el 25-esquema con las siguientes características.

Un vector aparece a lo más seis veces, por el caso 1; o un vector aparece a lo más $\lceil \frac{25}{12} \rceil = 3$ veces, por el caso 2. Sin perdida de generalidad, por las propiedades de equivalencia de los esquemas, supongamos que ese vector es $(0, 0) \, (mod \ 7)$.

Entonces tenemos al menos diecinueve puntos enteros diferentes del punto $(0,0)$ en $(mod\ 7)$; por el Lema 2.1 existen t de ellos, $1 \leq t \leq 7$, cuya suma es congruente con $(0,0)$ módulo 7. Claramente $t > 1$ y si $t = 7$ obtenemos la subsecuencia buscada. Si $2 \leq t \leq 6$, completamos la 7-linea en el 25-esquema con los vectores $(0,0)\,(mod\ 7)$ que ya teníamos. Esto completa la demostración.

□

2.4. Conjetura de Kemnitz

El análisis que hicimos anteriormente de algunos valores para la función $s(n,2)$ lo podemos resumir en la siguiente tabla.

n	s(n,2)
2	5=4(2)-3
3	9=4(3)-3
4	13=4(4)-3
5	17=4(5)-3
6	21=4(6)-3
7	25=4(7)-3

TABLA 3. Algunos valores para la función $s(n,2)$

Con esta información tenemos una conjetura, denominada la Conjetura de Kemnitz, que se enuncia de la siguiente manera:

Conjetura 2.1. Para todo número entero positivo n tenemos que:

$$s(n,2) = 4n - 3. \tag{2.8}$$

La reconstrucción de la prueba de esta conjetura es el principal resultado de este trabajo y como se mostró en el Teorema 2.5 es suficiente verificarla para el caso de $n = p$ primo.

CAPÍTULO 3

ALGUNAS COTAS PARA LA FUNCIÓN $s(p, 2)$

En este capítulo analizamos dos cotas relevantes que se estimaron para la función $s(n, 2)$, dadas por N. Alon y M. Dubiner [1] y L. Rónyai [38] y los diferentes argumentos que se utilizaron para la prueba de las mismas.

En primer lugar, describimos las cotas triviales que fueron dadas por H.Harbort [23] en el año de 1973, quien fue el primero que se interesó por estudiar la función más general $s(n, d)$, donde d es un entero positivo. En este caso el problema se enuncia de la siguiente manera:

Sea $\mathbb{Z}_n^d$ la suma directa de d copias del grupo aditivo $\mathbb{Z}_n$ de enteros módulo n, sea $s(n, d)$ el menor entero s tal que cualquier secuencia con s elementos de $\mathbb{Z}_n^d$ contiene una subsecuencia de tamaño n cuya suma de elementos es congruente con cero módulo n, el problema consiste en hallar $s(n, d)$ con la propiedad descrita.

Y las cotas triviales que garantizan la existencia de esta función son:

$$(n-1)2^d + 1 \leq s(n, d) \leq (n-1)n^d + 1. \tag{3.1}$$

Para el caso $d = 2$, la cota trivial inferior para la función $s(n, 2)$ es $4n - 3$ la prueba esta en que si tomamos una secuencia formada por $n - 1$ copias de cada uno de los cuatro puntos

$$(0, 0), (0, 1), (1, 0), (1, 1),$$

podemos observar que ninguna de las $\begin{pmatrix} 4n-4 \\ n \end{pmatrix}$ subsecuencias tiene suma cero.

La prueba de la cota trivial superior para la función $s(n,2)$ es la siguiente: consideremos una secuencia $\mathcal{P} = \{Q_1, \ldots, Q_{(n-1)n^2+1}\} \subseteq \mathbb{Z}_n \oplus \mathbb{Z}_n$ y la función $f : \mathcal{P} \to \mathbb{Z}_n \oplus \mathbb{Z}_n$ tal que:$f(Q_i) = Q_i$, para cada $i = 1, \ldots, (n-1)n^2 + 1$.

Por el Principio del Palomar al menos $\left\lceil \frac{(n-1)n^2+1}{n^2} \right\rceil = \left\lceil (n-1) + \frac{1}{n^2} \right\rceil = n$ puntos deben tener la misma imagen y por lo tanto la secuencia correspondiente a estos puntos tiene suma cero.

A continuación vamos a estudiar las cotas que se estimaron de la función $s(n,2)$, después de varios años de enunciar la conjetura; estas cotas son verificadas para el caso de n primo, al igual que el Teorema de Erdös, Ginzburg y Ziv y la Conjetura de Kemnitz.

La primera cota superior estimada para la función $s(p,2)$ fue dada por N. Alon y M. Dubiner [1], en el año de 1993; ellos probaron que $s(p,2) \leq 6p-5$ para cada p primo. Y más tarde, en el año de 1999, L. Rónyai [38] se acerca más al valor de la función, probando que $s(p,2) \leq 4p-2$. De aquí que, junto con la cota inferior, se tiene que el valor de $s(p,2)$ es $4p-3$ ó $4p-2$.

Recordemos que el Teorema de Chevalley-Warning es una herramienta fundamental para la prueba del Teorema de Erdös, Ginzburg y Ziv, en este caso tenemos el siguiente lema conocido como el Lema de Alon y Dubiner [1] como una aplicación del Teorema de Chevalley-Warning, el cual contribuye a la prueba de las dos cotas mencionadas anteriormente.

Lema 3.1. *Sea $\{\{v_1, \ldots, v_{3p}\}\}$ una secuencia en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ tal que*

$$\sum_{i=1}^{3p} v_i = (0,0). \tag{3.2}$$

Entonces existe un subconjunto $I \subset \{1, \ldots, 3p\}$ con $|I| = p$ tal que

$$\sum_{i \in I} v_i = (0,0). \tag{3.3}$$

Demostración. Sea $\{\{v_1, \ldots, v_{3p}\}\}$ una secuencia en $\mathbb{Z}_p \oplus \mathbb{Z}_p$, donde $v_i = (a_i, b_i)$, para cada $i = 1, \ldots, 3p$ y consideremos el siguiente sistema de polinomios definido por:

$$P_1(x_1, \ldots, x_{3p-1}) = \sum_{i=1}^{3p-1} a_i x_i^{p-1} = 0, \tag{3.4}$$

$$P_2(x_1, \ldots, x_{3p-1}) = \sum_{i=1}^{3p-1} b_i x_i^{p-1} = 0, \tag{3.5}$$

$$P_3(x_1, \ldots, x_{3p-1}) = \sum_{i=1}^{3p-1} x_i^{p-1} = 0, \tag{3.6}$$

donde P_1, P_2, $P_3 \in \mathbb{Z}_p[x_1, \ldots, x_{3p-1}]$.

Como cada polinomio es de grado $p-1$ y el número de variables es $3p-1$ tenemos

$$\sum_{i=1}^{3} grad(P_i) = 3(p-1) = 3p - 3 < 3p - 1.$$

Así, por el Teorema 1.4, el número N de soluciones del sistema es congruente con cero módulo p.

Ahora bien, como el vector nulo en $\mathbb{Z}_p^{3p-1}$ es una solución del sistema de polinomios entonces $N > 1$ y por consiguiente existe una solución no nula $(y_1, \ldots, y_{3p-1})$ con al menos un $y_j \neq 0$, $j \in \{1, \ldots, 3p-1\}$.

De aquí que,

$$P_1(y_1, \ldots, y_{3p-1}) = \sum_{i=1}^{3p-1} a_i y_i^{p-1} = 0, \tag{3.7}$$

$$P_2(y_1, \ldots, y_{3p-1}) = \sum_{i=1}^{3p-1} b_i y_i^{p-1} = 0, \tag{3.8}$$

$$P_3(y_1, \ldots, y_{3p-1}) = \sum_{i=1}^{3p-1} y_i^{p-1} = 0. \tag{3.9}$$

Luego, por el Pequeño Teorema de Fermat existe $J \subset \{1, \ldots, 3p-1\}$, de cardinalidad $|J| = p$ o $|J| = 2p$ tal que si sustituimos en (3.9), $\sum_{i \in J} y_i^{p-1} = 0$.

Por consiguiente, $\sum_{i \in J} a_i = 0$ y $\sum_{i \in J} b_i = 0$, o equivalentemente, $\sum_{i \in J} v_i = (0, 0)$.

Ahora, si $|J| = p$ entonces $I = J$, pero si este no es el caso; es decir, $|J| = 2p$, dado que por hipótesis $\sum_{i=1}^{3p} a_i = (0, 0)$, entonces $I = \{1, \ldots, 3p\} \setminus J$.

Esto completa la demostración. □

3.1. Cota estimada por N. Alon y M. Dubiner: $s(p,2) \leq 6p-5$

En esta sección presentamos la demostración de la cota estimada por N. Alon y M. Dubiner en [1] completando algunos detalles de las demostraciones. Consideremos la siguiente definición:

Definición 3.1. Sea $v = (d, e) \in \mathbb{Z}_p \oplus \mathbb{Z}_p$, definamos el vector de tamaño $(2p-2)$, $v^* = v^*(p)$, cuyas primeras $(p-1)$ coordenadas son todas d y las últimas $(p-1)$ coordenadas son e.

El siguiente lema es una consecuencia del Lema 1.3.

Lema 3.2. *Sean los vectores $v_1, \ldots, v_{2p-2}$ en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ y sea A la matriz de tamaño $(2p-2)\times(2p-2)$ cuyas columnas son $v_1^*, \ldots, v_{2p-2}^*$. Si en $\mathbb{Z}_p$, $per(A) \neq 0$, entonces para cualquier vector $b = (d, e) \in \mathbb{Z}_p \oplus \mathbb{Z}_p$, existen $\epsilon_1, \ldots, \epsilon_{2p-2}$ en $\{0, 1\}$ tales que* $b = \sum_{i=1}^{2p-2} \epsilon_i v_i$.

Demostración. Sea $c = (c_1, \ldots, c_{2p-2})$ un vector con entradas en $\mathbb{Z}_p$, cuyas primeras $p-1$ coordenadas son todas distintas de d y cuyas últimas $p-1$ coordenadas son todas distintas de e. Por el Lema 1.3, existen $\epsilon_1, \ldots, \epsilon_{2p-2}$ en $\{0, 1\}$ tales que para cada $1 \leq i \leq 2p-2$, la i-ésima coordenada de $\sum_{j=1}^{2p-2} \epsilon_j v_j^* \neq c_i$. Estas desigualdades, para $1 \leq i \leq p-1$, muestran que la primera coordenada de $\sum_{j=1}^{2p-2} \epsilon_j v_j$ es d, pues este elemento difiere de las primeras $p-1$ coordenadas de c. Análogamente, las desigualdades para $p \leq i \leq 2p-2$, muestran que la segunda coordenada de $\sum_{j=1}^{2p-2} \epsilon_j v_j$ es e, como queríamos demostrar. □

Ahora, consideremos la siguiente definición la cual será usada en la demostración del Lema 3.3.

Definición 3.2. Una *linea* en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ es el conjunto de todos los vectores

$$\{x + ty : t \in \mathbb{Z}_p\}, \tag{3.10}$$

donde x e y son dos vectores fijos en $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Cabe anotar que en algunos casos llamaremos a los elementos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ como puntos en lugar de vectores. Una característica interesante con esta definición es que para un subconjunto de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que no está contenido en una linea entonces contiene tres vectores u, v, w distintos, tales que el conjunto $\{u-w, v-w\}$ es una base de $\mathbb{Z}_p \oplus \mathbb{Z}_p$. La demostración la consignamos en el siguiente lema como un aporte a este trabajo.

Lema 3.3. *Si un subconjunto A de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ no está contenido en una linea entonces contiene tres vectores u, v, w distintos, tales que el conjunto $\{u-w, v-w\}$ es una base de $\mathbb{Z}_p \oplus \mathbb{Z}_p$.*

Demostración. Sea $A \subset \mathbb{Z}_p \oplus \mathbb{Z}_p$ que no está contenido en una linea entonces $|A| \geq 3$ puesto que:

- $A \neq \emptyset$ ya que el conjunto vacío es subconjunto de todo conjunto y por lo tanto está contenido en una linea,
- A no puede ser un conjunto unitario pues un vector cualquiera pertenece a una linea, y
- A no puede tener dos elementos pues con esos dos vectores podemos construir una linea.

Ahora bien, sean $v, w \in A$ distintos afirmamos que existe $u \in A$ tal que el conjunto $\{u-w, v-w\}$ es una base de $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Verifiquemos esta afirmación por contradicción.

Supongamos que el conjunto $\{u-w, v-w\}$ es linealmente dependiente, entonces para todo $u \in A$ tenemos que $u - w = \lambda(v-w),$ para algún $\lambda \in \mathbb{Z}_p$; lo cual es equivalente a

$$u = w + \lambda(v-w).$$

Luego, $A \subset \{v, w\} \cup \ell$ donde ℓ es el conjunto de puntos de la linea cuyos vectores fijos son $w, v-w$; es decir, $\ell = \{w + t(v-w) : t \in \mathbb{Z}_p\}$.

De aquí tenemos que, si $\lambda = 0$ implica que $w \in \ell$ y si $\lambda = 1$ implica que $v \in \ell$. Así, $A \subset \ell$, en contradicción. Por lo tanto, el conjunto $\{u-w, v-w\}$ es linealmente independiente y como su cardinalidad es igual a la dimensión del espacio, en este caso igual a 2, entonces este conjunto es una base de $\mathbb{Z}_p \oplus \mathbb{Z}_p$. □

Para la prueba de la cota estimada por Alon y Dubiner tenemos en cuenta el siguiente lema, demostrado por los mismos en [1].

Lema 3.4. *Sea S una secuencia de $6p-7$ vectores en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ y supongamos que ninguna linea contiene más de $2p-2$ elementos de S. Entonces existe una subsecuencia de $4p-4$ elementos de S, que los denotamos por $a_1, \ldots, a_{4p-4}$, tal que si $b_i = a_{2i} - a_{2i-1}$ para $1 \leq i \leq 2p-2$, y A es una matriz de tamaño $(2p-2) \times (2p-2)$ cuyas columnas son los vectores b_i^*, entonces $per(A) \neq 0$, en $\mathbb{Z}_p$.*

Demostración. Vamos a probar este lema por inducción sobre i.

Consideremos la base estándar $\{e_1, e_2\}$ de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ y sea A_0 una matriz de tamaño $(2p-2)\times(2p-2)$ cuyas primeras $(p-1)$ columnas son el vector e_1^* y cuyas últimas $(p-1)$ columnas son el vector e_2^*.

Claramente, $per(A_0) = ((p-1)!)^2 \neq 0 \, (mod \ p)$.

Ahora definimos los elementos $a_1, \ldots, a_{4p-4}$ secuencialmente, de tal manera que si definimos $a_1, \ldots, a_{2i}$ y $b_j = a_{2j} - a_{2j-1}$ para $1 \leq j \leq i$, tenemos lo siguiente: sea A_i la matriz que se obtiene de A_0 reemplazando en esta las primeras i columnas por las columnas $b_1^*, \ldots, b_i^*$, entonces en $\mathbb{Z}_p$, $per(A_i) \neq 0$.

Queremos verificar la existencia de A_{2p-2} tal que $per(A_{2p-2}) \neq 0$. Supongamos que $1 \leq i < 2p-2$ y que $a_1, \ldots, a_{2i}, b_1, \ldots, b_i$ y A_i se definieron igual que antes de tal manera que $per(A_i) \neq 0$, por hipótesis inductiva. El objetivo es definir $a_{2i+1}, a_{2i+2}, b_{i+1}$ y A_{i+1} con las propiedades requeridas.

Hagamos $S' = S \setminus \{a_1, \ldots, a_{2i}\}$, como $0 < i < 2p-2$ tenemos entonces que

$$|S'| \geq 6p - 7 - 2(2p-3) = 2p-1.$$

Por lo tanto, S' no está contenido en una linea y así contiene tres vectores u, v, w tales que el conjunto $\{u-w, v-w\}$ es una base de $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

De esto se sigue que la columna número $(i+1)$ de la matriz A_i es una combinación lineal de los permanentes de las dos matrices que se obtiene reemplazando estas $(i+1)$ columnas por $(u-w)^*$ y por $(v-w)^*$. Por lo tanto, al menos uno de estos dos permanentes, digamos el primero, es no nulo módulo p.

Podemos ahora definir $a_{2i+2} = u$ y $a_{2i+1} = w$, completando la demostración. □

En la siguiente proposición presentamos como en [1] que en efecto se cumple que:

$$s(p,2) \leq 6p-5. \tag{3.11}$$

Proposición 3.1. *Para un primo p y cualquier secuencia $\{\{a_1, \ldots, a_{6p-5}\}\}$ de elementos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$, existe $I \subset \{1, \ldots, 6p-5\}$, que satisface $|I| = p$ y*

$$\sum_{i \in I} a_i = (0,0). \tag{3.12}$$

Demostración. Sea S una secuencia de $6p-5$ elementos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$, supongamos primero que existen $2p-1$ elementos de S sobre la línea $\{x + ty : t \in \mathbb{Z}_p\}$, donde $x, y \in \mathbb{Z}_p \oplus \mathbb{Z}_p$ son fijos.

Sean $x + t_i y$, $1 \leq i \leq 2p-1$ éstos elementos. Por el Teorema 1.7 de Erdös, Ginzburg y Ziv, existe $I \subset \{1, \ldots, 2p-1\}$ tal que $|I| = p$ y $\sum_{i \in I} t_i = 0 (mod\ p)$. Por lo tanto, en $\mathbb{Z}_p \oplus \mathbb{Z}_p$,

$$\begin{aligned} \sum_{i \in I} (x + t_i y) &= \sum_{i \in I} x + \sum_{i \in I} t_i y \\ &= x \sum_{i \in I} 1 + y \sum_{i \in I} t_i \\ &= xp + y \sum_{i \in I} t_i \\ &= 0 \end{aligned}$$

completando la demostración en este caso (aquí 0 en $\mathbb{Z}_p \oplus \mathbb{Z}_p$).

Por consiguiente, podemos suponer que ninguna línea contiene más de $(2p-2)$ elementos de S. Por el Lema 3.4 podemos renumerar los elementos de S por $a_1, \ldots, a_{6p-5}$ y por lo tanto existe una subsecuencia de $4p-4$ elementos de S tal que si $b_i = a_{2i} - a_{2i-1}$ para $1 \leq i \leq 2p-2$, entonces el permanente de la matriz de tamaño $(2p-2) \times (2p-2)$ cuyas columnas son los vectores b_i^* es no nulo módulo p.

Por lo tanto, por el Lema 3.2 cada vector en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ es una combinación lineal de los vectores b_i con coeficientes en el conjunto $\{0, 1\}$.

En particular, existen $\epsilon_1, \ldots, \epsilon_{2p-2}$ en $\{0, 1\}$ tales que

$$\sum_{i=1}^{2p-2} \epsilon_i b_i = -a_1 - a_3 - \cdots - a_{4p-5} - a_{4p-3} - a_{4p-2} - a_{4p-1} - \cdots - a_{5p-2}.$$

Por la definición de los vectores b_i, obtenemos en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ que

$$a_{4p-3} + a_{4p-2} + a_{4p-1} + \cdots + a_{5p-2} + \sum_{i=1}^{2p-2} a_{2i-1} + \epsilon_i (a_{2i} - a_{2i-1}) = 0.$$

Por lo tanto, existe un subconjunto J de S tal que $|J| = 3p$ y cuya suma de sus elementos es 0, luego por el Lema 3.1, J contiene un subconjunto de tamaño p y suma cero, esto completa la demostración. □

3.2. Cota estimada por L. Rónyai: $s(p,2) \leq 4p-2$

Ahora presentamos la prueba de la cota estimada por L. Rónyai [38], para ello primero hacemos algunas observaciones.

Afirmamos que los monomios de la forma $\prod_{i\in I} x_i$, para $I \subseteq \{1,\ldots,m\}$, generan un espacio lineal de dimensión 2^m sobre un campo F.

En efecto, llamemos $J = \{1,\ldots,m\}$; como I es un conjunto que varia sobre el conjunto J, tenemos que el número total de subconjuntos I de J es $|\wp(J)| = 2^m$, donde $\wp(J)$ denota el conjunto de partes de J. Así, si $J = \{1,\ldots,m\}$ entonces I recorre los siguientes conjuntos:

$$\emptyset,\ \{1\},\ \{2\},\ \ldots\ ,\ \{m\},\ \{1,2\},\ \{1,3\},\ \ldots\ ,\ \{m-1,m\},\ \ldots\ ,\ \{1,2,\ldots,m\}.$$

Luego el conjunto de monomios que obtenemos es:

$$\{x_1, x_2, \ldots, x_m, x_1x_2, x_1x_3, \ldots, x_{m-1}x_m, \ldots, x_1x_2\cdots x_m\},$$

el cual junto con $1 \in F$ genera el espacio $F[x_1, x_2, \ldots, x_m]$.

Por otro lado, el conjunto de funciones características generan el espacio de las funciones definidas de $\{0,1\}^m$ en el campo F. En efecto, consideremos la función característica $\chi_u : \{0,1\}^m \to F$, definida por:

$$\chi_u(x) = \begin{cases} 1, & \text{si } x = u \\ 0, & \text{si } x \neq u \end{cases} \tag{3.13}$$

Dada una función $f : \{0,1\}^m \to F$ tenemos que esta función es una combinación lineal de las funciones características sobre F; pues si la función f toma el valor de $f(u)$ en el vector $u \in \{0,1\}^m$, entonces el coeficiente de $\chi_u(x)$ debe ser $f(u)$ en la expansión de f en términos de las funciones características.

Además, el conjunto de funciones características es linealmente independiente sobre F; pues si en una combinación lineal el coeficiente de $\chi_u(x)$ es c, con $c \neq 0$, entonces la combinación lineal no puede ser la función nula porque su valor en u es c.

Por lo tanto, el conjunto de funciones características forman una base del espacio de las funciones de $\{0,1\}^m$ en F.

Para la prueba de la cota superior estimada por L. Rónyai se usa el siguiente lema [38]:

Lema 3.5. *Sea F un campo y m un entero positivo. Entonces los monomios (multilineales) $\prod_{i\in I} x_i$, $I \subseteq \{1, 2, \ldots, m\}$, constituyen una base del espacio lineal de todas las funciones de $\{0,1\}^m$ en F, con coeficientes en el campo F. (Aquí 0 y 1 son elementos de F).*

Demostración. Como mencionamos anteriormente, el conjunto de monomios de la forma $\prod_{i\in I} x_i$, $I \subseteq \{1, \ldots, m\}$, generan el espacio $F[x_1, x_2, \ldots, x_m]$ cuya dimensión es 2^m. Además, esta es la dimensión del espacio de funciones de $\{0,1\}^m$ en F.

Como el conjunto de funciones características χ_u, $u \in \{0,1\}^m$ forman una base del espacio de funciones de $\{0,1\}^m$ en F, entonces es suficiente verificar que cada función característica es expresada como combinación lineal de los monomios $\prod_{i\in I} x_i$, con coeficientes en F.

Sea $u = (u_1, u_2, \ldots, u_m) \in \{0,1\}^m$ y sea $U \subseteq \{1, 2, \ldots, m\}$ el conjunto de indices j cuyas coordenadas $u_j = 1$ y el complemento de U, digamos $\overline{U}$, el conjunto de indices j con $u_j = 0$. Entonces tenemos

$$\chi_u(x_1, x_2, \ldots, x_m) = \prod_{j\in U} x_j \prod_{j\in\overline{U}} (1 - x_j) \tag{3.14}$$

como funciones de $\{0,1\}^m$.

Expandiendo el lado derecho de la ecuación (3.14) obtenemos una combinación lineal de los monomios de la forma $\prod_{i\in I} x_i$.

Además, como el conjunto de monomios es linealmente independiente, por la igualdad de polinomios, entonces los monomios (multilineales) $\prod_{i\in I} x_i$, $I \subseteq \{1, 2, \ldots, m\}$, constituyen una base del espacio lineal de todas las funciones de $\{0,1\}^m$ en F, con coeficientes en el campo F. □

Con las observaciones anteriores ya estamos listos para realizar la prueba de la cota superior estimada por L. Rónyai, el aporte se hace en esta prueba es el desarrollo en detalle de las afirmaciones que se presentan en la demostración de L. Rónyai [38].

Teorema 3.1. *Para cada primo p tenemos que:*

$$s(p, 2) \leq 4p - 2. \tag{3.15}$$

Demostración. Llamemos $m = 4p - 2$.

Sea $\{\{v_1, v_2, \ldots, v_m\}\}$ una secuencia en $\mathbb{Z}_p \oplus \mathbb{Z}_p$, donde cada v_i es de la forma $v_i = (a_i, b_i)$, para cada $i = 1, \ldots, m$.

Si p=2 entonces $m = 6$ y el resultado se tiene por la Proposición 2.1. Así que vamos a suponer que p es un número primo impar. Por el Lema 3.1 es suficiente probar que existe un subconjunto $J \subset \{1, \ldots, m\}$, con $|J| = 3p$ tal que $\sum_{j \in J} v_j = (0, 0)$.

Sea $\sigma(x_1, \ldots, x_m) := \sum_{I \subset \{1,\ldots,m\}, |I|=p} \prod_{i \in I} x_i$ el polinomio simétrico elemental p-ésimo en las variables $x_1, \ldots, x_m$. Y consideremos el polinomio P sobre el campo $\mathbb{Z}_p$ definido por:

$$P := P_1(x_1, \ldots, x_m) \cdot P_2(x_1, \ldots, x_m) \cdot P_3(x_1, \ldots, x_m) \cdot P_4(x_1, \ldots, x_m), \quad (3.16)$$

donde

$$P_1(x_1, \ldots, x_m) = \left(\sum_{i=1}^{m} a_i x_i \right)^{p-1} - 1, \quad (3.17)$$

$$P_2(x_1, \ldots, x_m) = \left(\sum_{i=1}^{m} b_i x_i \right)^{p-1} - 1, \quad (3.18)$$

$$P_3(x_1, \ldots, x_m) = \left(\sum_{i=1}^{m} x_i \right)^{p-1} - 1, \quad (3.19)$$

$$P_4(x_1, \ldots, x_m) = \sigma(x_1, \ldots, x_m) - 2. \quad (3.20)$$

Demostremos por contradicción el teorema. Supongamos que ningún subconjunto $J \subset \{1, \ldots, m\}$, $|J| = p$ o $|J| = 3p$ tiene suma cero.

Afirmamos que P se anula sobre todos los vectores no nulos $u \in \{0, 1\}^m$. En efecto, sea $u = (u_1, u_2, \ldots, u_m) \in \{0, 1\}^m$ no nulo, pueden suceder los siguientes casos

1. Si el número de unos del vector u es menor o igual que $p - 1$, entonces el factor P_3 se anula en u, luego $P(u) = 0$.
2. Si el número de unos del vector u es menor o igual que $2p - 1$, pero no p, entonces el factor P_3 se anula en u, pues si suponemos que $u_1 = \cdots, u_k = 1$, donde $k \in \{p + 1, \ldots, 2p - 1\}$ entonces

$$u_1 + u_2 + \cdots + u_p + u_{p+1} + \cdots + u_k + u_{k+1} + \cdots + u_m =$$
$$\underbrace{(1 + 1 + \cdots + 1)}_{p \text{ veces}} + \underbrace{(1 + 1 + \cdots + 1)}_{p-k \text{ veces}} + \underbrace{(0 + 0 + \cdots + 0)}_{2p-2+k \text{ veces}} =$$
$$0 + (1 + 1 + \cdots + 1) + 0 = p - k.$$

Luego $(u_1 + \cdots + u_m)^{p-1} = (p-k)^{p-1} = 1$ y así $P_3(u) = 0$. Por lo tanto $P(u) = 0$.

3. Análogamente, si el número de unos del vector u es menor o igual que $3p-1$ o $4p-2$, pero no p, $2p$ o $3p$, entonces el factor P_3 se anula en u, luego $P(u) = 0$.

4. Si el número de unos del vector u es $2p$ entonces el factor P_4 se anula en u, pues el número de términos no nulos de $\sigma(u)$ es $\begin{pmatrix} 2p \\ p \end{pmatrix}$ el cual es equivalente a 2 en $\mathbb{Z}_p$, por el Teorema 1.5 y por lo tanto $P(u) = 0$.

5. Si el número de unos del vector u es p , entonces en P el producto de P_1 y P_2 es cero sobre u. En efecto, consideremos $u_1 = \cdots = u_p = 1$ y las demás componentes ceros, tenemos entonces que

   $$P_1(u)P_2(u) = [(a_1+\cdots+a_p)^{p-1}-1][(b_1+\cdots+b_p)^{p-1}-1] = (A^{p-1}-1)(B^{p-1}-1),$$

   donde $A = a_1 + \cdots + a_p$ y $B = b_1 + \cdots + b_p$.

   Pueden suceder los siguientes casos:

   a) Si $A \neq 0$, implica que $A^{p-1} = 1$ y por lo tanto $P(u) = 0$.

   b) Si $B \neq 0$, implica que $B^{p-1} = 1$ y por lo tanto $P(u) = 0$.

   c) Si $A = 0$ y $B = 0$, entonces la secuencia $\{\{(a_1, b_1), \ldots, (a_p, b_p)\}\}$ tiene suma cero, en contradicción con lo supuesto. Luego este caso no se puede dar.

6. Por último, si el número de unos de u es $3p$, entonces en P el producto de P_1 y P_2 es cero sobre u. En efecto, consideremos $u_1 = \cdots = u_{3p} = 1$ y las demás componentes ceros, tenemos entonces que

   $$P_1(u)P_2(u) = [(a_1+\cdots+a_{3p})^{p-1}-1][(b_1+\cdots+b_{3p})^{p-1}-1] = (\widetilde{A}^{p-1}-1)(\widetilde{B}^{p-1}-1),$$

   donde $\widetilde{A} = a_1 + \cdots + a_{3p}$ y $\widetilde{B} = b_1 + \cdots + b_{3p}$.

   Al igual que en el caso anterior pueden suceder los siguientes casos:

   a) Si $\widetilde{A} \neq 0$, implica que $\widetilde{A}^{p-1} = 1$ y por lo tanto $P(u) = 0$.

   b) Si $\widetilde{B} \neq 0$, implica que $\widetilde{B}^{p-1} = 1$ y por lo tanto $P(u) = 0$.

   c) Si $\widetilde{A} = 0$ y $\widetilde{B} = 0$, entonces la secuencia $\{\{(a_1, b_1), \ldots, (a_{3p}, b_{3p})\}\}$ tiene suma cero y por el Lema 3.1 tenemos una contradicción, por tal razón este caso no se puede dar.

Por otro lado, tenemos que $P(0) = 2$.

De esta manera, podemos escribir P en términos de la función característica de la siguiente manera

$$P(u) = 2\chi_0(u),$$

donde, $\chi_0(u) = \begin{cases} 1 & \text{si } u = 0 \\ 0 & \text{si } u \neq 0 \end{cases}$

Notemos además que $grad(P) \leq 3(p-1) + p = 4p - 3$.

Ahora bien, si desarrollamos el lado derecho de la ecuación (3.16), se reduce P a una combinación lineal de monomios multilineales en las variables $x_1, \ldots, x_m$, usando la relación $x_i^2 = x_i$, lo cual es válido en $\{0,1\}^m$; llamemos Q a la expresión resultante.

Tenemos entonces que $Q(u) = 2\chi_0(u)$ es una función sobre $\{0,1\}^m$ y además $grad(Q) \leq 4p - 3$, pues la reducción no puede aumentar de grado. Pero esto es una contradicción, con la parte de la unicidad del Lema 4.3, por la representación multilineal de

$$2\chi_0(x_1, \ldots, x_m) = 2(1 - x_1)(1 - x_2) \cdots (1 - x_m) \tag{3.21}$$

que tiene grado $m = 4p - 2$. La contradicción establece el teorema. □

CAPÍTULO 4

PRUEBA DE LA CONJETURA DE KEMNITZ

En este capítulo vamos a presentar una reconstrucción de la prueba de la Conjetura de Kemnitz, con base en el artículo [37]; el aporte que hacemos en esta parte es la descripción en detalle de cada demostración de los resultados descritos por el autor C. Rehier en este artículo; en la primera sección se presentan cinco corolarios que tratan de algunas congruencias lineales que relacionan el número de subsecuencias de suma cero de una secuencia dada; como la herramienta principal que se utiliza para la prueba de estos corolarios es el Teorema de Chevalley-Warning, en algunos de ellos construimos los polinomios adecuados para la prueba de los mismos; en la segunda sección se presenta primero un lema conocido como el Lema de Reiher [37] el cual es la base de la demostración de la conjetura la cual se prueba por contradicción. Lo curioso de esta prueba es el ingenio que tiene el autor para establecer esas relaciones de congruencias lineales que lo llevan a la demostración de dicha conjetura.

Para la realización de estas pruebas enunciemos a continuación de nuevo el Teorema de Chevalley-Warning y el Lema de Alon y Dubiner presentados en los capítulos anteriores, para tenerlos presentes.

Teorema 4.1. *(Chevalley-Warning)*

Sean p un número primo impar y $\mathbb{F}_q$ el campo finito con $q = p^t$ elementos, donde t es un entero positivo. Para $i = 1, \ldots, m$, sean $P_i(x_1, \ldots, x_n)$ polinomios de grado d_i en n variables con coeficientes en $\mathbb{F}_q$.

Si $\sum_{i=1}^{m} d_i < n$ *entonces el número* N *de ceros comunes de* $P_1, \ldots, P_m$ *(en* $\mathbb{F}_q^n$*) satisface*

$$N \equiv 0 \,(\text{mod } p). \tag{4.1}$$

En particular, si existe un cero común entonces existe otro.

Como consecuencia de este teorema tenemos el Lema de Alon y Dubiner:

Lema 4.1. *Sea* $a_1, \ldots, a_{3p}$ *una secuencia en* $\mathbb{Z}_p \oplus \mathbb{Z}_p$ *tal que*

$$\sum_{i=1}^{3p} a_i = (0,0). \tag{4.2}$$

Entonces existe un subconjunto $I \subset \{1, \ldots, 3p\}$ *con* $|I| = p$ *tal que*

$$\sum_{i \in I} a_i = (0,0). \tag{4.3}$$

Como mostramos en el Capítulo 2 que la Conjetura es verdadera para el caso $p = 2$ entonces p lo tomamos en adelante como un número primo impar.

El símbolo $N(k, X)$ denota el número de subsecuencias de una secuencia dada $X \subset \mathbb{Z}_p \oplus \mathbb{Z}_p$ de cardinalidad k cuya suma de elementos es divisible entre p (o tiene suma cero) y $\sum X$ denotará la suma de todos los elementos de una secuencia X de $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

4.1. Resultados preliminares

Como mencionamos anteriormente, los resultados que siguen a continuación son dados por C. Rehier [37]. El primer corolario trata sobre la relación de congruencia lineal que existe entre la suma del número de subsecuencias de tamaños $p-1$, p, $2p-1$ y $2p$, de una secuencia dada. En el artículo [37] se presenta una idea de la demostración y aquí completamos los detalles.

Sea J a una secuencia de elementos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$, verifiquemos algunas congruencias lineales.

Corolario 4.1. *Si* $|J| = 3p - 3$ *entonces*

$$1 - N(p-1, J) - N(p, J) + N(2p-1, J) + N(2p, J) \equiv 0 \,(\text{mod } p). \tag{4.4}$$

Demostración. Sea $J = \{\{v_1, v_2, \ldots, v_{3p-3}\}\}$, donde $v_i = (a_i, b_i)$, para cada $i = 1, 2, \ldots, 3p-3$ y consideremos el siguiente sistema de los polinomios definido por:

$$P_1(x_1, \ldots, x_{3p-2}) = \sum_{n=1}^{3p-3} x_n^{p-1} + x_{3p-2}^{p-1} = 0, \tag{4.5}$$

$$P_2(x_1, \ldots, x_{3p-2}) = \sum_{n=1}^{3p-3} a_n x_n^{p-1} = 0, \tag{4.6}$$

$$P_3(x_1, \ldots, x_{3p-2}) = \sum_{n=1}^{3p-3} b_n x_n^{p-1} = 0, \tag{4.7}$$

donde P_1, P_2, P_3 en $\mathbb{Z}_p[x_1, \ldots, x_{3p-2}]$.

Dado que se cumplen las hipótesis del Teorema 4.1, tenemos que el número de soluciones N del sistema satisface $N \equiv 0\,(mod\ p)$.

Como el vector nulo es solución del sistema entonces $N > 0$ y N es múltiplo de p, así que: $N \geq p$.

A continuación vamos a contar los vectores no nulos que solucionan el sistema.

Consideremos $N(k, J) \neq 0$, los polinomios P_2 y P_3 se anulan en los vectores $u = (u_1, \ldots, u_{3p-2}) \in \mathbb{Z}_p^{3p-2}$ que tengan exactamente k componentes no nulas correspondientes a los índices de los elementos de las subsecuencias de tamaño k y suma cero.

Por ejemplo, si $N(k, J) = 1$ significa que existe una subsecuencia $I \subset J$ de tamaño k y suma cero, digamos (sin pérdida de generalidad) $\{\{v_1, \ldots, v_k\}\}$. Entonces los vectores $u \in \mathbb{Z}_p^{3p-2}$ que anulan los polinomios P_2 y P_3 son de la forma:

$$u = (u_1, \ldots, u_k, 0, \ldots, 0),$$

aquí $u_i \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. Por lo tanto, el número de vectores u de esta forma es $(p-1)^k$.

Ahora, si $N(k, J) = 2$ significa que existen dos subsecuencias distintas I_1, I_2 de J de tamaño k y suma cero, digamos $I_1 = \{\{v_1, \ldots, v_k\}\}$ e $I_2 = \{\{v_{i_1}, \ldots, v_{i_k}\}\}$, donde no necesariamente las subsecuencias son disjuntas. Entonces los vectores u y v en $\mathbb{Z}_p^{3p-2}$ que anulan los polinomios P_2 y P_3 son de la forma:

$$u = (u_1, \ldots, u_k, 0, \ldots, 0),$$

$$v = (v_1, \ldots, v_{3p-2})$$

donde

$$v_i = \begin{cases} u_{i_j} & \text{si } i = j \\ 0 & \text{en otro caso} \end{cases}$$

aquí $u_i, u_{i_j} \in \mathbb{Z}_p^*$.

El número de vectores de esta forma es:

$$(p-1)^k + (p-1)^k = 2(p-1)^k = (p-1)^k N(k, J).$$

Por lo tanto, si tenemos $N(k, J) > 0$ subsecuencias de tamaño k y suma cero, el número de vectores $u \in \mathbb{Z}_p^{3p-2}$ que anulan los polinomios P_2 y P_3 es

$$(p-1)^k N(k, J).$$

Ahora vamos a contar el número de soluciones comunes de los polinomios P_1, P_2 y P_3.

El polinomio P_1 se anula en los vectores $u = (u_1, \ldots, u_{3p-2}) \in \mathbb{Z}_p^{3p-2}$ que tengan p ó $2p$ componentes no nulas; el número de estos vectores es:

$$\begin{pmatrix} 3p-2 \\ p \end{pmatrix} (p-1)^p + \begin{pmatrix} 3p-2 \\ 2p \end{pmatrix} (p-1)^{2p}.$$

Pero como en este caso queremos contar el número de vectores u que anulan los tres polinomios, para ello vamos a considerar dos casos: la última componente del vector u es nula o no; es decir, $u_{3p-2} = 0$ ó $u_{3p-2} \neq 0$.

- Si $u_{3p-2} = 0$ entonces el número de vectores u que anulan los tres polinomios es:

$$\begin{aligned} N_1 &= (p-1)^p N(p, J) + (p-1)^{2p} N(2p, J) \\ &\equiv -N(p, J) + N(2p, J) (mod\ p), \end{aligned}$$

- Si $u_{3p-2} \neq 0$ entonces el número de vectores u que anulan los tres polinomios es:

$$\begin{aligned} N_2 &= (p-1)^p N(p-1, J) + (p-1)^{2p} N(2p-1, J) \\ &\equiv -N(p-1, J) + N(2p-1, J) (mod\ p). \end{aligned}$$

En el último caso, las secuencias que anulan los polinomios deben tener tamaño $p-1$ o $2p-1$, pues ya tenemos una componente no nula, para el polinomio P_1.

Luego, contando la solución nula, el número total de soluciones del sistema de polinomios es:

$$\begin{aligned} N &= 1 + N_1 + N_2 \\ &= 1 - N(p-1, J) - N(p, J) + N(2p-1, J) + N(2p, J) \\ &\equiv 0 \, (mod\ p). \end{aligned}$$

□

El siguiente corolario, análogamente al anterior, trata sobre la relación de congruencia lineal que existe entre la suma del número de subsecuencias de tamaños p y $2p$, pero en este caso la secuencia dada tiene tamaño $3p-2$ o $3p-1$. La demostración es análoga a la anterior.

Corolario 4.2. *Si* $|J| = 3p-2$ *o* $|J| = 3p-1$ *entonces*

$$1 - N(p, J) + N(2p, J) \equiv 0 \,(\text{mod } p). \tag{4.8}$$

Demostración. Sea $J = \{\{v_1, \ldots, v_{3p-2}\}\}$, donde $v_i = (a_i, b_i)$, $i = 1, \ldots, 3p-2$ y consideremos el siguiente sistema de polinomios definido por:

$$P_1(x_1, \ldots, x_{3p-2}) = \sum_{n=1}^{3p-2} x_n^{p-1} = 0, \tag{4.9}$$

$$P_2(x_1, \ldots, x_{3p-2}) = \sum_{n=1}^{3p-2} a_n x_n^{p-1} = 0, \tag{4.10}$$

$$P_3(x_1, \ldots, x_{3p-2}) = \sum_{n=1}^{3p-2} b_n x_n^{p-1} = 0, \tag{4.11}$$

donde P_1, P_2, P_3 en $\mathbb{Z}_p[x_1, \ldots, x_{3p-2}]$.

Dado que se cumplen las hipótesis del Teorema 4.1, tenemos que el número de soluciones N del sistema satisface que $N \equiv 0 \,(mod\ p)$.

Como el vector nulo es solución del sistema entonces $N > 0$ y N es múltiplo de p, así que: $N \geq p$. Análogamente al Corolario 4.2, vamos a contar los vectores no nulos que solucionan el sistema.

El polinomio P_1 se anula en un vector $u = (u_1, \ldots, u_{3p-2})$ si existen exactamente p ó $2p$ componentes no nulas; como el vector u también debe anular los polinomios P_2 y P_3 entonces el total de vectores que son solución del sistema es:

$$\begin{aligned} N &= 1 + (p-1)^p N(p, J) + (p-1)^{2p} N(2p, J) \\ &\equiv 1 - N(p, J) + N(2p, J) \,(mod\ p). \end{aligned}$$

Análogamente se demuestra la congruencia cuando $|J| = 3p-1$, definiendo el anterior sistema de polinomios con la diferencia que ahora P_1, P_2 y P_3 son polinomios que pertenecen a $\mathbb{Z}_p[x_1, \ldots, x_{3p-1}]$.

□

El corolario que sigue es una consecuencia de los anteriores, con una hipótesis adicional.

Corolario 4.3. *Si* $|J| = 3p-2$ *o* $|J| = 3p-1$, *entonces* $N(p,J) \equiv 0 (\text{mod } p)$ *implica que*

$$N(2p, J) \equiv -1 \,(\text{mod } p). \tag{4.12}$$

Demostración. Se sigue del Corolario 4.2. □

Ahora llamemos X a una secuencia de elementos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$. En el resultado que se muestra a continuación tenemos un aporte para este trabajo ya que la demostración no aparece en el artículo mencionado; este aporte radica en la construcción de los polinomios adecuados para contar el número de subsecuencias de suma cero y de esta manera poder verificar las relaciones de congruencia dadas.

Corolario 4.4. *Si* $|X| = 4p-3$ *entonces*

$$-1 + N(p,X) - N(2p,X) + N(3p,X) \equiv 0 \,(\text{mod } p) \tag{4.13}$$

y

$$N(p-1,X) - N(2p-1,X) + N(3p-1,X) \equiv 0 \,(\text{mod } p). \tag{4.14}$$

Demostración. Sea $X = \{\{v_1, \ldots, v_{4p-3}\}\}$, donde $v_i = (a_i, b_i)$, $i = 1, \ldots, 4p-3$. Para la prueba de la congruencia (4.13), consideremos el siguiente sistema de polinomios definido por:

$$P_1(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} x_n^{p-1} = 0, \tag{4.15}$$

$$P_2(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} a_n x_n^{p-1} = 0, \tag{4.16}$$

$$P_3(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} b_n x_n^{p-1} = 0, \tag{4.17}$$

donde P_1, P_2, P_3 en $\mathbb{Z}_p[x_1, \ldots, x_{4p-3}]$.

Observe que la suma de los grados de los tres polinomios es $3p-3$, la cual es estrictamente menor que el número de variables $4p-3$, por el Teorema 4.1 tenemos que el número de soluciones N del sistema satisface $N \equiv 0 \,(mod\ p)$.

Como el vector nulo es solución del sistema entonces $N > 0$ y N es múltiplo de p, así que: $N \geq p$.

Ahora contemos las soluciones no nulas del sistema; el polinomio P_1 se anula en un vector $u = (u_1, \ldots, u_{4p-3})$ con exactamente p, $2p$ ó $3p$ componentes no nulas. Como queremos además que el vector u anule los polinomios P_2 y P_3 entonces el número de vectores u que hacen esto, es:

$$\begin{aligned} N_1 &= (p-1)^p N(p,X) + (p-1)^{2p} N(2p,X) + (p-1)^{3p} N(3p,X) \\ &\equiv -N(p,X) + N(2p,X) - N(3p,X) \,(mod\ p). \end{aligned}$$

Luego, el total de soluciones del sistema es:

$$\begin{aligned} N &= 1 - N(p,X) + N(2p,X) - N(3p,X) \\ &\equiv -1 + N(p,X) - N(2p,X) + N(3p,X) \\ &\equiv 0 \,(mod\ p). \end{aligned}$$

Para la prueba de la congruencia (4.14), consideremos el siguiente sistema de polinomios definido por:

$$P_1(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} x_n^{p-1} + 1 = 0, \tag{4.18}$$

$$P_2(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} a_n x_n^{p-1} = 0, \tag{4.19}$$

$$P_3(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} b_n x_n^{p-1} = 0, \tag{4.20}$$

donde P_1, P_2, P_3 en $\mathbb{Z}_p[x_1, \ldots, x_{4p-3}]$.

Como la suma de los grados de los tres polinomios es $3p-3 < 4p-3$ (número de variables), por el Teorema 4.1 tenemos que el número de soluciones N del sistema satisface $N \equiv 0 \,(mod\ p)$.

Para que el polinomio P_1 se anule en un vector $u = (u_1, \ldots, u_{4p-3})$; este vector debe tener exactamente $p-1$, $2p-1$ o $3p-1$ componentes no nulas ya que por suposición tenemos la última componente no nula. Además estos vectores deben anular los polinomios P_2 y P_3 entonces el número de vectores que hacen esto es:

$$N = (p-1)^{p-1} N(p-1,X) + (p-1)^{2p-1} N(2p-1,X) + (p-1)^{3p-1} N(3p-1,X),$$

$$N \equiv N(p-1,X) - N(2p-1,X) + N(3p-1,X) \,(mod\ p).$$

□

Lo interesante de la siguiente demostración es que además de usar el argumento algebraico que veníamos utilizando también se usan argumentos combinatorios de conteo. Aquí completamos los detalles de la demostración.

Corolario 4.5. *Si* $|X| = 4p-3$ *entonces*

$$3 - 2N(p-1,X) - 2N(p,X) + N(2p-1,X) + N(2p,X) \equiv 0 \,(\text{mod } p). \quad (4.21)$$

Demostración. Sea X una secuencia con $4p-3$ elementos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Vamos a considerar todas las subsecuencias I de X de tamaño $3p-3$; por el Corolario 4.1, cada subsecuencia I satisface

$$1 - N(p-1,I) - N(p,I) + N(2p-1,I) + N(2p,I) \equiv 0 \,(mod\ p).$$

Ahora bien, si sumamos todas las congruencias lineales sobre cada subsecuencia I de X obtenemos:

$$\sum_{I\subset X,|I|=3p-3} [1 - N(p-1,I) - N(p,I) + N(2p-1,I) + N(2p,I)] \equiv 0 \,(mod\ p),$$

$$\sum_{I\subset X,|I|=3p-3} 1 - \sum_{I\subset X,|I|=3p-3} N(p-1,I) - \sum_{I\subset X,|I|=3p-3} N(p,I) +$$

$$\sum_{I\subset X,|I|=3p-3} N(2p-1,I) + \sum_{I\subset X,|I|=3p-3} N(2p,I) \equiv 0 \,(mod\ p),$$

$$\binom{4p-3}{3p-3} - \binom{3p-2}{2p-2} N(p-1,X) - \binom{3p-3}{2p-3} N(p,X) +$$

$$\binom{2p-2}{p-2} N(2p-1,X) + \binom{2p-3}{p-3} N(2p,X) \ \equiv\ 0 \,(mod\ p),$$

$$\binom{3p+(p-3)}{2p+(p-3} - \binom{2p+(p-2)}{p+(p-2)} N(p-1,X) \ -$$

$$\binom{2p+(p-3)}{p+(p-3)} N(p,X) + \binom{p+(p-2)}{p-2} N(2p-1,X) \ +$$

$$\binom{p+(p-3)}{p-3} N(2p,X) \ \equiv\ 0 \,(mod\ p),$$

por el Teorema 1.5 obtenemos que:

$$\begin{pmatrix} 3 \\ 2 \end{pmatrix}\begin{pmatrix} p-3 \\ p-3 \end{pmatrix} - \begin{pmatrix} 2 \\ 1 \end{pmatrix}\begin{pmatrix} p-2 \\ p-2 \end{pmatrix} N(p-1,X) -$$

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix}\begin{pmatrix} p-3 \\ p-3 \end{pmatrix} N(p,X) + \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} p-2 \\ p-2 \end{pmatrix} N(2p-1,X) +$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} p-3 \\ p-3 \end{pmatrix} N(2p,X) \equiv 0 \ (mod\ p),$$

así,

$$3 - 2N(p-1,X) - 2N(p,X) + N(2p-1,X) + N(2p,X) \equiv 0\,(mod\ p).$$

□

4.2. Prueba de la Conjetura de Kemnitz

En esta sección se presenta un lema dado por C. Rehier en [37] que es la base fundamental de la prueba de la conjetura así como las relaciones de congruencias estudiadas en la sección anterior; en este lema completamos los detalles de la demostración.

Recordemos que se denotará por $\sum X$ a la suma de todos los elementos de una secuencia X de $\mathbb{Z}_p \oplus \mathbb{Z}_p$. El lema que sigue se conoce con el nombre de Lema de Reiher [37] el cual es muy útil para la prueba de la Conjetura de Kemnitz hoy Teorema de Reiher.

Lema 4.2. *(Lema de Reiher)*

Si $|X| = 4p-3$ *y* $N(p,X) = 0$ *entonces*

$$N(p-1,X) \equiv N(3p-1,X)\,(\text{mod } p). \tag{4.22}$$

Demostración. Consideremos la siguiente partición de la secuencia X;

$X = A \cup B \cup C$, donde $|A| = p-1$, $|B| = p-2$ y $|C| = 2p$ y tales que:

$$\sum A \equiv (0,0)(\text{mod } p), \quad \sum B \equiv \sum X(\text{mod } p), \quad \sum C \equiv (0,0)\,(\text{mod } p).$$

Llamemos χ al número de particiones de la secuencia X con las anteriores características; vamos a determinar χ en módulo p.

Tenemos que $|X \setminus A| = 3p - 2$, como por hipótesis $N(p, X) = 0$ también lo es $N(p, X \setminus A)$, luego por el Corolario 4.3 tenemos que:

$$N(2p, X \setminus A) \equiv -1 \, (mod \text{ p}).$$

Si recorremos sobre todas las posibles subsecuencias A tenemos que

$$\begin{aligned} \chi &= \sum_{A} N(2p, X \setminus A) \\ &\equiv \sum_{A} -1 \, (mod \text{ p}) \\ &\equiv -N(p-1, X) \end{aligned}$$

Por otro lado, tenemos que $|X \setminus B| = 3p - 1$, como por hipótesis $N(p, X) = 0$ también lo es $N(p, X \setminus B)$, luego por el Corolario 4.3 tenemos que

$$N(2p, X \setminus B) \equiv -1 \, (mod \text{ p}).$$

Si recorremos sobre todas las posibles subsecuencias B tenemos que

$$\begin{aligned} \chi &= \sum_{B} N(2p, X \setminus B) \\ &\equiv \sum_{B} -1 \, (mod \text{ p}). \end{aligned}$$

Como $\sum B \equiv \sum X$ entonces $\sum X \setminus B \equiv (0, 0) \, (mod \text{ p})$.

Luego,

$$\begin{aligned} \sum_{B} 1 &= |\{B \subset X : \textstyle\sum B \equiv \sum X\}| \\ &= |\{B \subset X : \textstyle\sum X \setminus B \equiv (0,0) \, (mod \text{ p})\}| \\ &= |\{Y \subset X : |Y| = 3p-1, \textstyle\sum Y \equiv (0,0) \, (mod \text{ p})\}| \\ &= N(3p-1, X). \end{aligned}$$

Luego, $\chi \equiv -N(3p - 1, X) \, (mod \text{ p})$.

En consecuencia de lo anterior tenemos que $N(p-1, X) \equiv N(3p-1, X)(mod \text{ p})$.

□

Por último, tenemos la demostración de la Conjetura de Kemnitz, dada por C. Reiher [37].

Teorema 4.2. *(Teorema de Reiher)*

Cualquier secuencia de $4p-3$ *elementos de* $\mathbb{Z}_p \oplus \mathbb{Z}_p$ *contiene una subsecuencia de cardinalidad* p *y suma cero.*

Demostración. Hagamos la prueba por contradicción. Sea X una secuencia de $4p-3$ puntos enteros del plano y supongamos que ninguna subsecuencia de tamaño p de X tiene suma cero. Es decir que $N(p, X) = 0$ Sumando las congruencias (4.13), (4.14) y (4.21) tenemos que

$$\begin{gathered} -1 + N(p, X) - N(2p, X) + N(3p, X) + \\ N(p-1, X) - N(2p-1, X) + N(3p-1, X) + \\ 3 - 2N(p-1, X) - 2N(p, X) + N(2p-1, X) + N(2p, X) = \\ 2 - N(p-1, X) + N(3p-1, X) + N(3p, X) \equiv 0 \,(mod \text{ p}). \end{gathered}$$

Como $N(p, X) = 0$ por el Lema 4.2 $N(p-1, X) \equiv N(3p-1, X) \,(mod \text{ p})$ entonces

$$2 - N(p-1, X) + N(3p-1, X) + N(3p, X) = 2 + N(3p, X) \,(mod \text{ p}).$$

Así,

$$2 + N(3p, X) \equiv 0 \,(mod \text{ p}).$$

Por lo tanto, $N(3p, X)$ debe ser no nulo; luego existe por lo menos una subsecuencia de X de tamaño $3p$ y suma cero; por consiguiente, por el Lema 4.1 existe una subsecuencia de tamaño p y suma cero, en contradicción con lo supuesto.

Por lo tanto, $N(p, X) \neq 0$. □

CONCLUSIONES

- En este trabajo presentamos cuatro demostraciones del Teorema de Erdös, Ginzburg y Ziv, el cual fue el punto de partida del estudio de los problemas de suma cero; el objetivo de presentar las cuatro demostraciones fue para estudiar los diferentes argumentos utilizados ya que están relacionados con el estudio de las cotas estimadas para la función $s(n, 2)$ y la prueba de la Conjetura de Kemnitz; lo curioso de esta prueba es que se utilizan herramientas algebraicas, como el Teorema de Chevalley-Warning, para probar este tipo de problemas combinatorios los argumentos algebraicos no son suficientes para la prueba, la utilización de herramientas algebraicas y combinatorias se convierten en una herramienta muy poderosa.

- Verificamos que la conjetura es verdadera para algunos casos particulares, usando la función $s(n, 2)$ definida por:

$$s(n, 2) := \text{mín}\{|\mathcal{P}| : \mathcal{P} \subset \mathbb{Z} \times \mathbb{Z} \text{ y } \mathcal{P} \text{ tiene suma cero}\}.$$

- Realizamos el estudio de los casos $n = 2$, 3, 5 y 7 en detalle. Para el estudio del caso $n = 7$ realicé los cálculos puesto que no aparecen en la literatura estudiada, donde calculé las diferentes formas de la primera fila de los s-esquemas que pueden ocurrir y la tabla de la función $A_7(s, t)$ y con estos datos comprobé que si se cumple la conjetura para $n = 7$.

- Además, se realizó la reconstrucción de la prueba de la Conjetura de Kemnitz con base en el artículo *On Kemnitz'conjeture concerning lattice-points in the plane.* Ramanujan J., *13:333-337, 2007* de *Christian Reiher*. El aporte que se hace en este trabajo es la ampliación, verificación y descripción en detalle

de cada demostración de los resultados dados por el autor C. Rehier; en particular se presentan cinco corolarios que tratan de algunas congruencias lineales que relacionan el número de subsecuencias de suma cero de una secuencia dada; como la herramienta principal que se utiliza para la prueba de estos corolarios es el Teorema de Chevalley-Warning, en algunos de ellos construí los polinomios adecuados para la prueba de los mismos, los cuales no aparecen reportados en la literatura.

- Los problemas de suma cero es un tema de frontera en la investigación actual ya que a partir de ellos surge la Teoría de Suma Cero; tiene aplicaciones en muchos aspectos de campos finitos y Teoría de Grafos [46] y también tienen relación con los conjuntos suma, los cubrimientos de enteros, la Teoría de Ramsey y Teoría de Códigos.

Perspectivas.

- Aunque se han realizado estudios del problema inicial para dimensiones mayores que dos, solamente se han logrado ciertas cotas para la función $s(n,d)$, con $d>2$; por ejemplo, la cota superior fue mejorada en gran medida por N. Alon y M. Dubiner en [2] probando que $s(n,d)\leq c(d)n$, donde $c(d)$ es una constante independiente de n. Su demostración usa propiedades de expansión de grafos de Cayley y Teoría de Números Aditiva. C. Elsholtz en [13] prueba que la constante $c(d)\geq 2^d 1{,}125^{\lfloor \frac{d}{3} \rfloor}$. Para enteros compuestos $n=n_1n_2$, una cota superior de $s(n,d)$ fue estimada por H. Harborth [23] la cual depende de los valores de $s(n_1,d)$ y $s(n_2,d)$ así:

  $$s(n,d)=s(n_1n_2,d)\leq \text{mín}\{s(n_1,d)+(s(n_2,d)-1)n_1, s(n_2,d)+(s(n_1,d)-1)n_2\}.$$

  De igual manera, se han realizado muchos estudios sobre el valor de la función $s(n,d)$ para ciertos casos particulares; por ejemplo: $s(3,3)=19$, $s(3,4)=41$, $s(3,5)=91$ y se ha logrado estimar ciertas cotas para $s(3,d)$ con $d\geq 5$, podemos remitirnos a [6, 13, 45].

- Otros problemas afines son el estudio de la Constante de Davenport y la Constante de Olson para grupos en general ya que para ciertos grupos en particular, como los p-grupos, ya se conocen sus valores y también estudiar la relación entre ellas y la relación que tienen con la función $s(n,d)$.

Bibliografía

[1] N. Alon and M. Dubiner. *Zero-sum sets of prescribed size.* Combinatorics, Paul Erdös is Eighty, János Bolyai Math Soc.,Budapest (1993), 33-50.

[2] N. Alon and M. Dubiner. *A lattice point problem and additive number theory.* Combinatorica 15 (1995), 301-309. János Bolyai Math Soc.,Budapest (1993), 33-50.

[3] N. Alon, N. Linial and R. Meshulam. *Additive Bases of Vector Spaces over Prime Fields.* J. Combinatorial Theory, Ser. A, 57 (1991), 203-210.

[4] N. Alon. *Tools from Higher Algebra.* Esto aparece en: "Handbook in Combinatorics", R. L. Graham, M. Grötschel and L. Lovás eds., North Holland. (1986)

[5] A. Blokhuis. *Polynomials in finite geometries and combinatorics*, Proc. 14^{th} British Combinatorial Conference, London Mathematical Society Lecture Notes Series 187, edited by K. Walker, Cambridge University Press (1993), 35-52.

[6] C. Brewbaker. *Lower Bound Visualization of a Zero-Sum Problem.* Iowa State University (2002).

[7] A. Cauchy. Recherches sur les nombres, J. Ecole Polytech, Volume 9 (1813), 99-116.

[8] Y. Caro. *Zero.-sum problems-A Survey.* Discrete Mathematics 152 (1996), 93-113.

[9] C. Chevalley. "French: Démonstration dúne hypothése de M. Artin". Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 11: 73-75. Zbl 0011.14504 JFM 61.1043.01. (French), (1936).

[10] P. Clark. *The Chevalley-Warning Theorem (Featuring. . .The Erdös-Ginzburg-Ziv Theorem)*. Manuscrito.

[11] H. Davenport. *On the addition of residue classes*, Journal of the London Mathematical Society, Volume 10, 1935, Pág. 30-32.

[12] R. Eggleton y P. Erdös. *Two Combintorial Problems in Group Theory* Acta Arithmetica, 21 (1972), 111-116.

[13] C. Elsholtz. *Lower bounds for multidimensional zero sum*. Combinatorica 24 (3) (2004), 351-358.

[14] P. Erdös, A. Ginzburg and A. Ziv. *Theorem in the Additive Number Theory*. Bull Research Council, Israel 10F (1961), 41-43.

[15] M. Erickson. *Introduction to Combinatorics*. Jhon Wiley & Sons, Inc, United States of America (1963).

[16] W. Gao. *Two Addition Theorems on Groups of Prime Order*. Journal of Number Theory 56 (1996), 211-213.

[17] W. Gao. *Any* $2n-1$ *integers contain exactly* n *integers whose sum is a multiple of* n, J. of Northeast Normal University 4 (1985).

[18] W. Gao. *Note on a zero sum problem*, J. Combinatorial Theory , Ser. A, 95(2001), 387-389.

[19] R. Guy. *Unsolved Problems in Number Theory*. Springer Science Business Media, Inc, New York, (2004).

[20] M. Hall. *Combinatorial theory*, Blaisdell (1967).

[21] H. Halberstam and K. F. Roth. (1983). *Sequences* (revised ed.). Berlin: Springer-Verlag. ISBN 9780387908014.

[22] Y. Hamidoune, O. Ordaz and A. Ortunio. *On a combinatorial theorem of Erdös-Ginzburg and Ziv*. Combinatorics, Probability and Computing 7 (1998), 403-412.

[23] H. Harborth. *Ein Extremalproblem für Gitterpunkte*. J. Reine Angew. Math, 262/263 (1973), 356-360.

[24] A. Kemnitz. On a lattice point problem, Ars Combinatorica 16b (1983), 151-160.

[25] H. Mann. *Two Addition Theorems*. Journal Combinatorial Theory 3, 233-235, 1967.

[26] H. Minc. *Nonnegative matrices*, Wiley (1988).

[27] H. Minc. *Permanents*, Addison-Wesley (1978).

[28] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, New York, 1997.

[29] M. Nathanson. *Additive Number Theory. Inverse Problems and The Geometry of Sumsets*. Springer-Verlag, New York, 1996.

[30] J. Olson. *An addition theorem modulo p*. J. Combinatorial Theory 5 (1968), 45-52.

[31] J. Olson. *A Combinatorial Problem on Finite Abelian Groups I*. Journal Number Theory 1 (1969), 8-11.

[32] J. Olson. *A Combinatorial Problem on Finite Abelian Groups II*.Journal Number Theory 1 (1969), 195-199.

[33] J. Olson. *On a combinatorial problem of Erdös, Ginzburg, and Ziv*. Journal of Number Theory 8 (1976), Issue 1, 52-57.

[34] A. Plagne and W. Schmid. *An Application of Coding Theory to Estimating Davenport Constants*. Sometida a publicación.

[35] O. Ramaré. *On snirel man's constant*. Annali della Scuola Normale Superiore di Pisa. Classe di Science. Serie IV 22(4) (1995), 645-706.

[36] T. Redmond and C. Ryavec. *The Mathematical Intelligencer* 2 (1980), 106.

[37] C. Reiher. *On Kemnitz'conjeture concerning lattice-points in the plane*. Ramanujan J. 13 (2007), 333-337.

[38] L. Rónyai. *On a Conjeture of Kemnitz*. Combinatorica 20 (2000), 569-573.

[39] H.J. Ryser. *Combinatorial mathematics*, Wiley and Math. Assoc. Amer. (1963).

[40] H. J. Ryser and R. A. Brualdi. *Combinatorial Matrix Theory*, Cambridge University Press, New York (1991).

[41] S. Savchev and F. Chen. *Kemnitz'conjeture revisited*. Discrete Mathematics 297 (2005), 196-201.

[42] T. Tao and V.H. Vu. *Additive Combinatorics*. Cambridge University Press, New York (2006).

[43] E. Warning. “Comment on the preceding work of Mr. Chevalley (German: Bemerkung zur vorstehenden Arbeit von Herrn Chevalley)”. Abhand. Mathe. Sem. Hamburg 11: 76-83. Zbl 0011.14601 JFM 61.1043.02. (German), 1936.

[44] Zhi-Wei Sun and Jian-Xin Liu. *A Note on the Erdös, Ginzburg, Ziv Theorem.* Nanjing Univ. J. Natur. Sci. 37(2001), N° 4, 473-476.

[45] Zhi-Wei Sun. *A Survey of Zero-Sum Problems on Abelian Groups.* Nanjin 210093.

[46] Zhi-Wei Sun. *Unification of zero-sum problems subsets sums and covers of* $\mathbb{Z}$. Electronic Research Annoncements of the American Mathematical Society 9 (2003), 51-60.